UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NORTH CAROLINA
CHARLOTTE DIVISION

J.R. and J.S., *individually and on behalf of all others similarly situated*, Plaintiffs, vs. ATRIUM HEALTH, INC., Defendant.	Case No.: **DEMAND FOR JURY TRIAL**

CLASS ACTION COMPLAINT

Plaintiffs J.R. and J.S. ("**Plaintiffs**"), individually and on behalf of all others similarly situated, bring this class action lawsuit against Defendant Atrium Health, Inc. ("**Atrium**" and/or "**Defendant**"). Plaintiffs' allegations are based upon personal knowledge as to themselves and their own acts, and upon information and good faith belief as to all other matters based on the investigation conducted by undersigned counsel.

INTRODUCTION

1. This case seeks legal redress for Defendant's conscious decision to install tracking technologies on its website to collect its patients' personal health information and disclose that highly sensitive information to third party platforms like Facebook and Google without consent.

2. Defendant Atrium is a healthcare organization and hospital network offering a wide range of clinical services to patients across multiple states.[1] Defendant operates 40 hospitals, 7 emergency departments, 30 urgent care centers and approximately 1400 additional care locations

[1] *Atrium Health 2019 Annual Report,* https://atriumhealth.org/files/build_annual_report/index.html

throughout North Carolina, South Carolina, Georgia and Alabama. According to Atrium, it has approximately 34,000 patient encounters every day across these locations.[2]

3. In order to market, sell and provide its healthcare offerings, Defendant owns, maintains and operates a website, https://atriumhealth.org/ (the "**Website**"), and a patient portal, https://my.atriumhealth.org/myatriumhealth (the "**Portal**" and collectively with the Website, the "**Web Properties**").

4. As detailed herein, Defendant disregarded the privacy rights of its patients who used its Web Properties ("**Users**" or "**Class Members**") by installing, configuring and using pixels and other tracking technologies on its Web Properties to collect and divulge their personally identifiable information ("**PII**") and protected health information ("**PHI**" and collectively, "**Private Information**") to Meta Platform Inc. d/b/a Facebook and other social media platforms.

5. Unbeknownst to Users and without their authorization or informed consent, Defendant installed Facebook's Meta Pixel ("**Meta Pixel**" or "**Pixel**") and other invisible third-party tracking technology on its Web Properties in order to intercept Users' PII and PHI with the express purpose of disclosing that Private Information to third parties such as Meta and/or Google LLC in violation of HIPAA Privacy Rule and 42 U.S.C. § 1320d-6 as well as state, federal and common law.

6. Meta then accesses and uses the Private Information by associated it with the individual User whose information was disclosed to create targeted advertising that it sends to that User's personal Facebook account. Meta is able to personally identify each User with an active Facebook account by using the "c_user" cookie that Meta stores in users' browsers and which reveals a Facebook account-holder's unique "FID" value.

[2] *Id.*

7. A user's FID is linked to their Facebook profile which personally identifies the user through a wide range of demographic and other information about the user including the User's name, pictures, personal interests, work history, relationship status and other details. Because the user's FID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the FID to quickly and easily locate, access, and view the user's corresponding Facebook profile.[3]

8. Notably, the Pixel collects data regardless of whether the User has a Facebook account as Facebook maintains "shadow profiles" on users without Facebook accounts and links the information collected via the Pixel to the user's real-world identity using their shadow profile.[4]

9. The screenshots of Defendant's website, more fully explained *infra*, demonstrate how the Meta Pixel intercepts Users' Private Information including the Private Information of Plaintiffs and Class Members. For example, a tool called the "Meta Pixel Helper" allows individuals to see whether Defendant is using Meta Pixels on its Website including specific "events" the Pixels are set up to capture (for instance, which page is visited, or which buttons are clicked by website visitors). The Meta Pixel helper is a tool Meta intended for its customers—like Defendant—to use to verify that the Pixel is working properly, troubleshoot common errors and improve Pixel performance.[5]

10. Depending on the browser they are using, customers and others can also inspect the

---

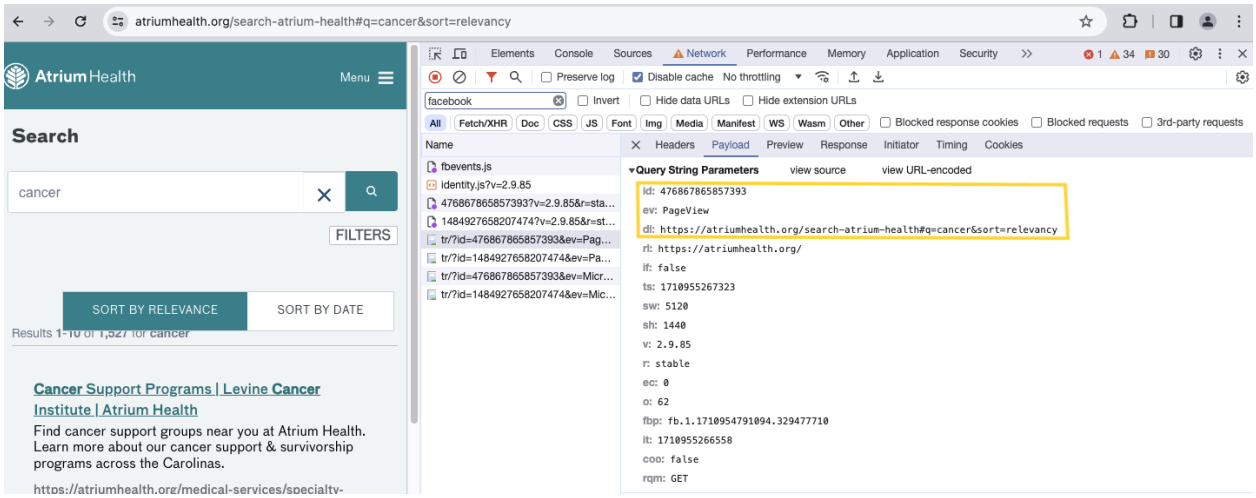
[3] To find the Facebook account associated with a particular c_user cookie, one simply needs to type www.facebook.com/ followed by the c_user ID.

[4] *See* Russell Brandom, *Shadow Profiles Are The Biggest Flaw In Facebook's Privacy Defense*, TheVerge.com (Apr 11, 2018), *available at* https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (last visited Apr. 4, 2024).

[5] https://developers.facebook.com/docs/meta-pixel/support/pixel-helper/ (last accessed March 13, 2024).

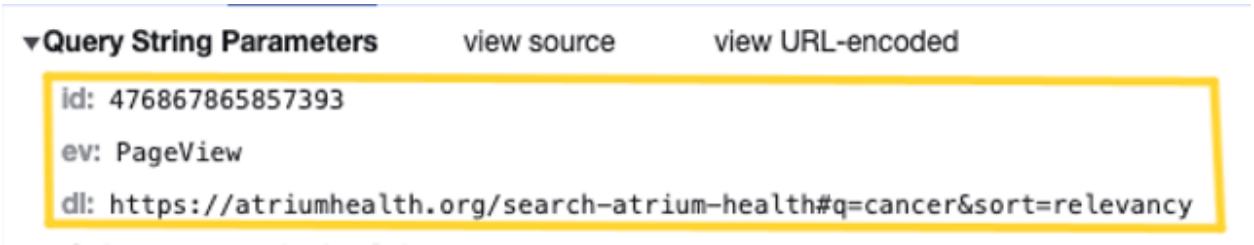
"source code" of a particular website (in Google Chrome this can be done by "right-clicking" on a webpage and selecting "inspect" from the menu that appears) to view the performance of the Pixel in order to see what information Defendant is disclosing to Meta for each webpage a User is visiting.

11. Data privacy experts are also capable of viewing how the Meta Pixel operates on various websites, including past configurations, and expert analysis demonstrates how Atrium used the Pixels on its Web Properties, in particular. The first screenshot below shows what a webpage from Defendant's Web Properties looks like when you use the Meta Pixel Helper or similar tools in order to see how the Pixel works to disclose information to Meta.



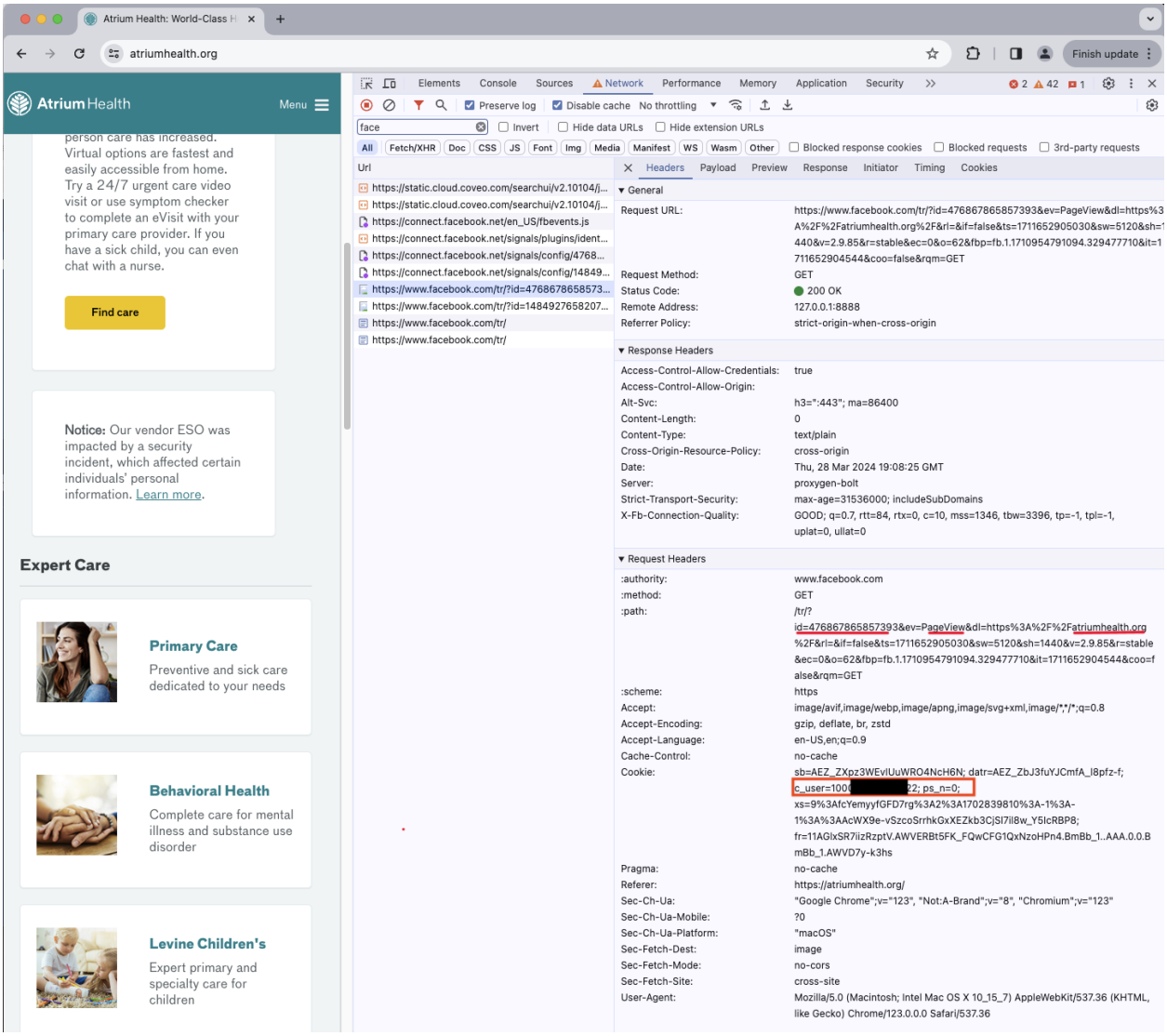
12. On the left-hand side of the screenshot is the page as it appears to any User visiting this webpage. This is the result the User would see if they went to Atrium's search bar, typed in "cancer" and pressed Enter. There are 1,527 matches for that search on Defendant's Website.

13. The right-hand side of the screenshot, also displayed below, is through the use of the Google Chrome "Inspect" tool to reveal what information Defendant is disclosing to Meta through the Pixel in the background and unbeknownst to the User.



14. Essentially, Defendant discloses the exact terms of patients' search queries on its Website via the "search bar" function.

15. Below are larger images of the Meta pixel in action. Though it appears to be code, a closer inspection makes it apparent that Defendant is disclosing both personally identifiable information in the form of the c_user FID, which uniquely identifies an individual's Facebook



account (as well as other cookies that Facebook is known to utilize to identify individuals).

16. The highlighted portions show some of the categories of information that Defendant is sharing with Meta. Beginning at the top, the "id=4768…" is the unique ID number of one of the Pixels installed by Defendant. Next to that is "PageView," a type of 'event' collected by the Pixel as the User navigates the Website which shares the URL of the page that the User is visiting.[6] Finally, on the top line, Defendant is disclosing that the User is visiting "atriumhealth.org." As demonstrated by the images below and as Plaintiffs' research showed, Defendant discloses the descriptive URL of any treatment-specific page visited next (for example, https://atriumhealth.org/medical-services/prevention-wellness/behavioral-health or https://atriumhealth.org/medical-services/prevention-wellness/womens-health/maternity-services#classes), type of provider sought (for example, "obstetrics and gynecology" via https://atriumhealth.org/find-a-doctor/results?new_patient=true&skill=specialty-33-obstetrics-and-gynecology&sort=best_match), or the fact that the patient is making an appointment (for example, via https://atriumhealth.org/make-an-appointment).

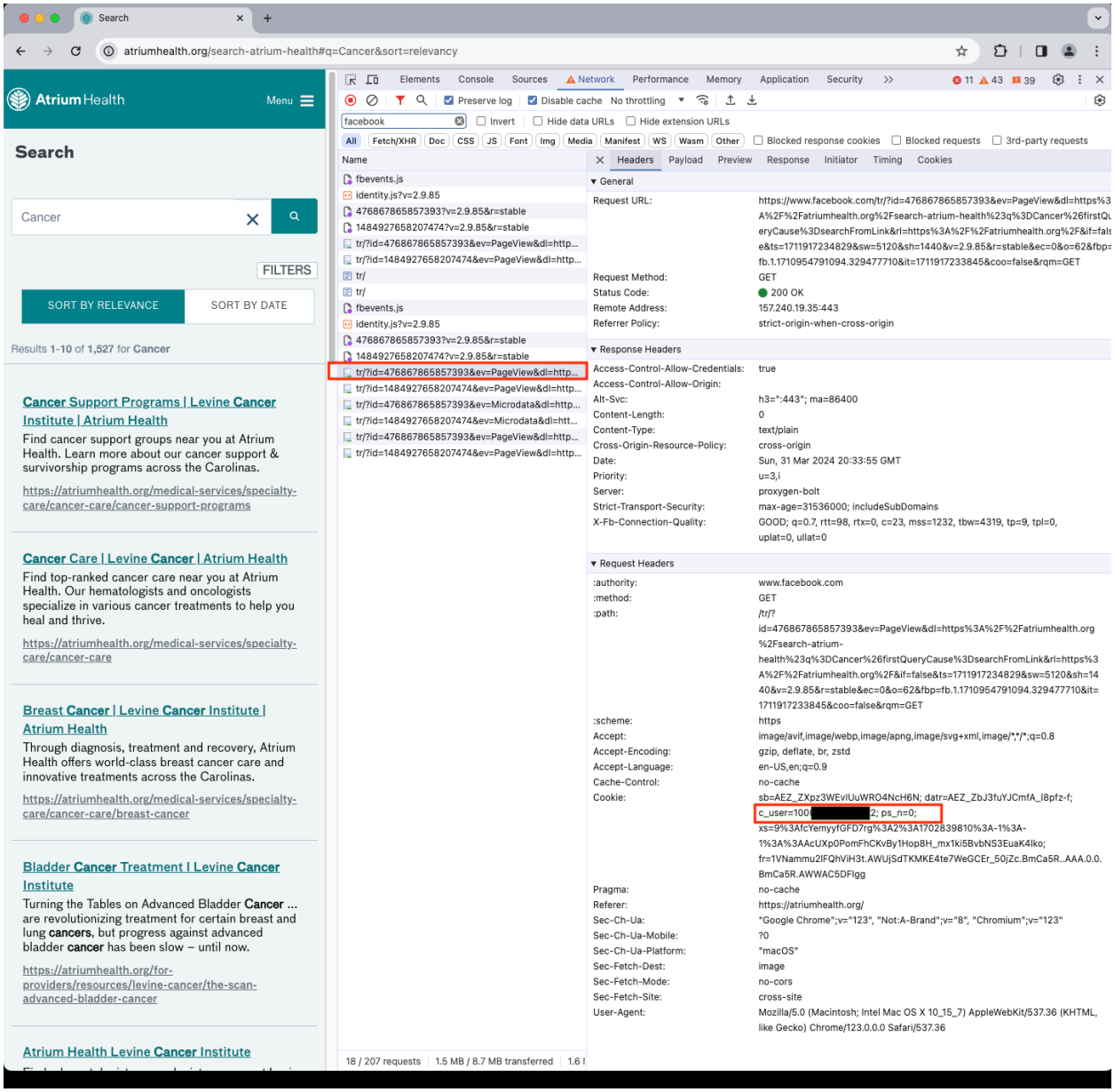
17. In the image below, Defendant is disclosing to Meta the PHI of the User.

18. Specifically, Defendant is disclosing that the User performed a "search" and the "keywords" they typed in for that search were "cancer."

19. As the page loads, the Meta Pixel triggers the "PageView" event, automatically sending information such as the webpage URL – which contains the User's exact search keywords – to Meta. Now Meta knows that the User is searching for information related to the condition and

[6] A URL is the web address that your type in the address bar at the top of the screen or which appear in the address bar when you click on a link. It stands for Uniform Resource Locator. When you go to use google, the URL that appears is google.com. And when you click on google maps, the URL changes to google.com/maps. It is that extension to the URL, "maps" that provides additional pageview information that allows pixels and trackers to know more about your internet usage.

treatment of cancer, personal health information that is protected by HIPAA.



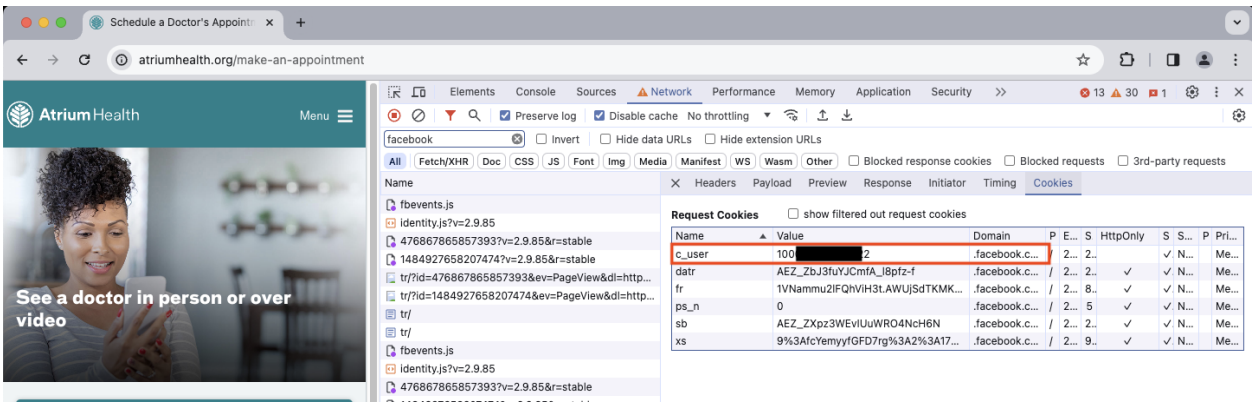
20. The line which begins with "Cookie" contains the PII disclosed to Meta that allows Meta to specifically associate the PHI shared in the earlier lines with a specific individual.

21. The first highlighted term is the "c_user" cookie followed by a number which contains the unique Facebook User ID for the person who is visiting this webpage.

22. This user ID, or FID, can be used to easily find the Facebook account of any user.

If you have a person's FID (for example, FID 12345), all you have to do is add it to the Facebook URL to find the profile. In our example, it would be: facebook.com/12345.

23. The image below shows some of the Facebook cookies which contain unique personal identifiers that the Meta Pixel collects along with patients' PHI that get disclosed to Meta (here, when the patient is attempting to make an appointment):



24. The first one is the c_user cookie. The second is a "datr" cookie which contains a unique alphanumeric code and identifies the specific web browser from which the User is sending the communication. It is an identifier that is unique to the User's web browser and is therefore a means of identification for Meta. Meta keeps a record of every datr cookie identifier associated with each of its users.

25. The third is the "fr" cookie, a unique combination of the c_user and datr cookies.

26. Meta, at the very least, uses c_user, datr, and fr cookies to identify individual Facebook users and track their activity across the internet.

27. Expert analysis has determined that Atrium had active Pixels on its Web Properties from at least 2017 until at least October 2022. Using the Pixels installed on its Web Properties, Atrium transmitted PageView, Microdata, and SubscribedButtonClick events about Users' activities.

28. Upon a User's arrival on Atrium's homepage, Atrium immediately sent a pair of

PageView and Microdata events to Facebook revealing that the User was on the page, "https://www.atriumhealth.org/."

29. As Users navigated beyond the homepage, Atrium continued to disclose User data including Users': (i) keyword search activities; (ii) appointment activities; (iii) medical conditions and treatment sought; (iv) patient status, and (v) MyChart login activities, at the very least.

30. Atrium used the Pixel to track Plaintiffs and Class Members when they made appointments with specific providers, as well. This is indicated by the exemplary screenshots below, which show how the action of clicking "Make an Appointment" (via a "SubscribedButtonClick" event set up by Atrium that captures the text of buttons clicked by Users) was transmitted to Meta simultaneously with the user's FID (contained within the c_user cookie, redacted for this public filing) and prior searches for "cancer."

31. In other words, when the User made an appointment with a healthcare provider at Atrium, their unique, personally identifiable FID, linked to their medical need for a specific healthcare appointment, was disclosed to Meta, thereby transmitting PHI to Meta.


```
:authority:          www.facebook.com
:method:             GET
:path:               /tr/?
                     id=1484927658207474&ev=SubscribedButtonClick&dl=https%3A%2F%2Fat
                     riumhealth.org%2Fsearch-atrium-
                     health%23q%3DCancer%26sort%3Drelevancy&rl=https%3A%2F%2Fatrium
                     health.org%2F&if=false&ts=1711917293225&cd[buttonFeatures]=%7B%22cl
                     assList%22%3A%22clickNavigationTracking%22%2C%22destination%22%3
                     A%22https%3A%2F%2Fatriumhealth.org%2Fmake-an-
                     appointment%22%2C%22id%22%3A%22%22%2C%22imageUrl%22%3A%2
                     2%22%2C%22innerText%22%3A%22Make%20an%20Appointment%22%2C
                     %22numChildButtons%22%3A0%2C%22tag%22%3A%22a%22%2C%22typ
                     e%22%3Anull%2C%22name%22%3A%22%22%7D&cd[buttonText]=Make%
                     20an%20Appointment&cd[formFeatures]=%5B%5D&cd[pageFeatures]=%7B
                     %22title%22%3A%22%5Cn%20%20%20%20%20%20%20%20%20%20%2
                     0%20%20%20%20%20Search%5Cn%20%20%20%20%20%20%20%20%2
                     0%20%20%20%22%7D&cd[parameters]=%5B%5D&sw=5120&sh=1440&v=
                     2.9.85&r=stable&ec=3&o=30&fbp=fb.1.1710954791094.329477710&it=17119
                     17233845&coo=false&es=automatic&tm=3&rqm=GET
:scheme:             https
Accept:              image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
Accept-Encoding:     gzip, deflate, br, zstd
Accept-Language:     en-US,en;q=0.9
Cache-Control:       no-cache
Cookie:              sb=AEZ_ZXpz3WEvlUuWRO4NcH6N; datr=AEZ_ZbJ3fuYJCmfA_l8pfz-f;
                     c_user=100[redacted]2; ps_n=0;
                     xs=9%3AfcYemyyfGFD7rg%3A2%3A1702839810%3A-1%3A-
                     1%3A%3AAcUXp0PomFhCKvBy1Hop8H_mx1ki5BvbNS3EuaK4lko;
                     fr=1VNammu2lFQhViH3t.AWUjSdTKMKE4te7WeGCEr_50jZc.BmCa5R..AAA.0.
                     0.BmCa5R.AWWAC5DFlgg
```

32. In other words, by using the Pixels it installs on its Web Properties, Defendant intercepts both the PII and the PHI of every User that visits every webpage, with the specific purpose of disclosing that HIPAA-protected health information to Meta.

33. Meta, which created the Pixel and assigns a unique FID to each of its Facebook account holders, knows how to combine the information intercepted and shared by Defendant so that Meta can connect each User to the PHI that is disclosed. Meta does this in order to send targeted ads related to the medical conditions and treatments each User shares with Defendant to that User's personal Facebook account.

34. The Pixel intercepts and discloses the information of every Facebook user that visits the Defendant's Web Properties in the same way.

35. When Plaintiffs and Class Members visited Defendant's Web Properties, the URLs that describe the medical information on each page they visited (for example: https://atriumhealth.org/locations/detail/atrium-health-pulmonology-university-city) and/or the search terms they typed in Defendant's search bar were simultaneously shared with Meta during every interaction.

36. And together with that PHI, Defendant's Pixel (which relies on Facebook cookies to function) discloses to Meta the Facebook user ID of every person that visits its Web Properties so that Meta can personally identify that user and that user's PHI – including Plaintiffs and every Class Member who visited Defendant's Web Properties to research and share HIPAA-protected health information with Defendant while the Pixel was installed on the Web Properties.

37. Plaintiffs and Class Members who visited and used Defendant's Web Properties thought they were communicating with only their trusted healthcare providers, and reasonably

believed that their sensitive and private PHI would be guarded with the utmost care. In browsing Defendant's Web Properties—be it to make an appointment, locate a doctor with a specific specialty, find sensitive information about their diagnosis, or investigate treatment for their diagnosis—Plaintiffs and Class Members did not expect that every search (including exact words and phrases they typed into Defendant's website search bars), extremely sensitive PHI such as health conditions (e.g., breast cancer or pregnancy), diagnoses (e.g., stroke, arthritis, or AIDS), procedures sought, treatment status, and/or their treating physician, or even their access/interactions on Defendant's online Portal would be intercepted, captured and otherwise shared with Facebook in order to target Plaintiffs and Class Members with ads, in conscious disregard of their privacy rights.

38. Plaintiffs continued to have their privacy violated when their Private Information was used to turn a profit by way of targeted advertising related to their respective medical conditions and treatments sought.

39. Defendant knew that by embedding the Meta Pixel on its Web Properties it was permitting Facebook to collect and use Plaintiffs' and Class Members' Private Information, including sensitive medical information.

40. Defendant (or any third parties) did not obtain Plaintiffs' and Class Members' prior consent before sharing their sensitive, confidential communications with third parties such as Facebook.

41. Defendant's actions constitute an extreme invasion of Plaintiffs' and Class Members' right to privacy and violate federal and state statutory and common law as well as Defendant's own Privacy Policies that affirmatively and unequivocally state that any personal

information provided to Defendant will remain secure and protected.[7]

42. As a result of Defendant's conduct, Plaintiffs and Class Members have suffered numerous injuries, including: (i) invasion of privacy; (ii) lack of trust in communicating with doctors online; (iii) emotional distress and heightened concerns related to the release of Private Information to third parties; (iv) loss of the benefit of the bargain; (v) diminution of value of the Private Information; (vi) statutory damages and (vii) continued and ongoing risk to their Private Information.

43. Plaintiffs and Class Members have a substantial risk of future harm, and thus injury in fact, due to the continued and ongoing risk of misuse of their Private Information that was shared by Defendant with unauthorized third parties.

44. Plaintiffs seek, on behalf of themselves and a class of similarly situated persons, to remedy these harms and therefore assert the following statutory and common law claims against Defendant: (i) Violation of Electronic Communications Privacy Act, 18 U.S.C. §2511(1), *et seq*; (ii) Negligence; (iii) Breach of Express Contract, (iv) Breach of Implied Duty of Good Faith and Fair Dealing, (v) Breach of Implied Contract, (vi) Breach of Fiduciary Duty and (vii) Unjust Enrichment.

PARTIES

45. Plaintiff J.R. is a Michigan citizen, residing in Oakland County, Michigan, where she intends to remain indefinitely. Plaintiff J.R. was a patient of Atrium between September 2007 and 2011 as well as between September 2020 and October 2023, and has been using its Web

[7] Atrium's Privacy Policies (and other affirmative representations) represent to Users that it will not share Private Information with third parties without the patient's consent. *See* https://atriumhealth.org/for-patients-visitors/privacy (last visited Apr. 4, 2024).

Properties since at least September 2020. Plaintiff J.R. was a resident of Watauga County, North Carolina during the relevant times until she moved to Michigan in or about October 2023.

46. Plaintiff J.S. is and at all relevant times was, a North Carolina resident, residing in Forsyth County, North Carolina. Plaintiff J.S. has been a patient of Atrium since 2007 and has used its Web Properties since Atrium introduced its Portal.

47. Defendant Atrium Health, Inc. is a healthcare service provider. Defendant is incorporated in Delaware with its principal place of business located at 1000 Blythe Blvd., Charlotte, North Carolina 28203.

JURISDICTION & VENUE

48. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C § 1332(d), because the amount in controversy for the Class exceeds $5,000,000 exclusive of interest and costs, there are more than one hundred (100) putative class members defined below, and minimal diversity exists because a significant portion of putative class members are citizens of a state different from the citizenship of at least one Defendant.

49. Pursuant to 28 U.S.C. Section 1391, this Court is the proper venue for this action because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District. At least one Plaintiff resides in this District and used Defendant's Web Properties within this District. Moreover, Defendant received substantial compensation from offering healthcare services in this District, and Defendant made numerous misrepresentations which had a substantial effect in this District, including, but not limited to, representing that it will only disclose Private Information provided to them under certain circumstances, ***which do not*** include disclosure of Private Information for marketing purposes.

50. Defendant is subject to personal jurisdiction in North Carolina because Defendant maintains its principal place of business in North Carolina and is authorized to conduct and is conducting business in North Carolina.

REPRESENTATIVE PLAINTIFFS' EXPERIENCES

A. Plaintiff J.R.

51. Plaintiff J.R. has been a patient of Defendant since approximately 2006 and has utilized Defendant's Web Properties since at least September 2020.

52. As a condition of receiving Defendant's services, Plaintiff J.R. disclosed her Private Information to Defendant on numerous occasions, and most recently in October 2023.

53. Plaintiff J.R. accessed Defendant's Web Properties on her phone and computer to receive healthcare services from Defendant and at Defendant's direction.

54. Plaintiff J.R. has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

55. During the relevant time period (when the Defendant's Pixels were present) Plaintiff J.R. used Defendant's Website, https://www.atriumhealth.org/, to research pulmonology, neurology, interventional radiology; research doctors, schedule appointments, understand test results, and join support groups; look for Defendant's locations close to their address including Defendant's emergency room departments and COVID testing locations.

56. In 2020, Plaintiff J.R. was diagnosed with a neurological and a pulmonary condition and submitted information to Defendant's Web Properties about her condition and treatments received, as well as schedule appointments to receive those treatments.

57. Shortly after submitting her protected health information including information concerning their specific symptoms and treatments to Defendant, Plaintiff J.R. began to receive spam and ads on Facebook and other social media related to medications and prescriptions.

58. Upon information and good faith belief, Plaintiff J.R. began receiving these ads after her PII and PHI concerning her medical condition was disclosed by Defendant through the Pixel to Meta, such as for medications and prescriptions related to her conditions.

59. Meta viewed and accessed this Private Information so that it could personally identify Plaintiff J.R. by connecting the c_user FID to their Facebook account. Meta also accesses the PHI disclosed by Defendant so that it can use the specific medical information Plaintiff J.R. shared with Defendant to identify specific targeted ads related to Plaintiff J.R.'s medical condition to send to their Facebook account. After accessing and identifying the specific medical conditions it can target with ads, Meta then shares that information with other unauthorized third parties whose businesses and advertisements are related to those conditions.

60. The full scope of Defendant's interceptions and disclosures of Plaintiff J.R.'s communications to Meta can only be determined through formal discovery. However, Defendant intercepted at least the following communications about Plaintiff J.R.'s patient status, medical knee condition, treatments sought, and prospective specialized healthcare providers, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff J.R.'s specific medical conditions, queries, as well as types of providers and treatments sought):

- https://atriumhealth.org/search-atrium-health#q=pulmonology&sort=relevancy
- https://atriumhealth.org/search-atrium-health#q=neurology&sort=relevancy

- https://atriumhealth.org/search-atrium-health#q=interventional%20radiology&sort=relevancy
- https://atriumhealth.org/search-atrium-health#q=er&sort=relevancy
- https://atriumhealth.org/locations/emergency-departments
- https://atriumhealth.org/find-a-doctor

61. Contemporaneously with the interception and transmission of the contents of Plaintiff J.R.'s communications regarding her conditions on https://www.atriumhealth.org/, Defendant also disclosed to Meta Plaintiff J.R.'s unique personal identifiers, including but not limited to, her Facebook ID and IP address.

62. During the relevant time period, when the Defendant's Pixels were present, Plaintiff J.R. also utilized Defendant's Patient Portal to review her medical records such as her visit summaries, doctor's notes and her test results.

63. The full scope of Defendant's interceptions and disclosures of Plaintiff J.R.'s communications to Meta can only be determined through formal discovery.

64. However, upon information and good faith belief, Defendant intercepted at least the following communications about Plaintiff J.R.'s patient status, via the following URLs or substantially similar URLs were sent to Meta via the Pixel, indicating that Plaintiff J.R. is a patient of Defendant who is about to use the patient portal:

- https://my.atriumhealth.org/myatriumhealth/authentication/login

65. Plaintiff J.R. reasonably expected that her communications with Defendant via the Web Properties were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

66. Plaintiff J.R. provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

67. As described herein, Defendant worked along with Facebook to intercept Plaintiff J.R.'s communications, including those that contained her Private Information.

68. Defendant willfully facilitated these interceptions without Plaintiff J.R.'s knowledge, consent or express written authorization.

69. Defendant transmitted to Facebook Plaintiff's Facebook ID, computer IP address and sensitive health information such as her medical symptoms, conditions, treatments sought, physician selected, button/menu selections and/or content typed into free text boxes.

70. By doing so without her consent, Defendant breached Plaintiff J.R.'s privacy and unlawfully disclosed her Private Information.

71. Defendant did not inform Plaintiff J.R. that it had shared her Private Information with Facebook.

72. Plaintiff J.R. would not have utilized Defendant's medical services and/or used its Web Properties or would have paid much less for Defendant's services had she known that her Private Information would be captured and disclosed to third parties like Facebook without her consent.

B. Plaintiff J.S.

73. Plaintiff J.S. has been a patient of Defendant since approximately 2007 and has utilized Defendant's Web Properties since on or about 2007.

74. As a condition of receiving Defendant's services, Plaintiff J.S. disclosed her Private Information to Defendant on numerous occasions, and most recently in 2024.

75. Plaintiff J.S. accessed Defendant's Web Properties on her phone and computer to receive healthcare services from Defendant and at Defendant's direction.

76. Plaintiff J.S. has used and continues to use the same devices to maintain and access an active Facebook account throughout the relevant period in this case.

77. During the relevant time period (when the Defendant's Pixels were present) Plaintiff J.S. used the search bar embedded on Defendant's Website, https://www.atriumhealth.org/, to research vision issues and treatments (ocular HSD). Additionally, Plaintiff J.S. used the site to locate an alcohol rehabilitation center. Further, she used the Web Properties to research doctors, schedule appointments, understand test results, upload insurance information, and join support groups; look for Defendant's locations close to their address including Defendant's emergency departments and COVID testing locations.

78. Shortly after submitting her protected health information including information concerning her specific symptoms and treatments to Defendant, Plaintiff J.S. began to receive spam and ads on Facebook and other social media related to her specific health conditions.

79. Upon information and good faith belief, Plaintiff J.S. began receiving these ads after her PII and PHI concerning her medical conditions were disclosed by Defendant through the Pixel to Meta.

80. Meta viewed and accessed this Private Information so that it could personally identify Plaintiff J.S. by connecting the c_user FID to their Facebook account.

81. Meta also accesses the PHI disclosed by Defendant so that it can use the specific medical information Plaintiff J.S. shared with Defendant to identify specific targeted ads related to Plaintiff J.S.'s medical condition to send to their Facebook account.

82. After accessing and identifying the specific medical conditions it can target with ads, Meta then shares that information with other unauthorized third parties whose businesses and advertisements are related to those conditions.

83. The full scope of Defendant's interceptions and disclosures of Plaintiff J.S.'s communications to Meta can only be determined through formal discovery.

84. However, Defendant intercepted at least the following communications about Plaintiff J.S.'s patient status, various vision/eye issues, treatments sought, and prospective specialized healthcare providers, via the following long-URLs or substantially similar URLs that were sent to Meta via the Pixel (and which contain information concerning Plaintiff J.S.'s specific medical conditions, queries, as well as types of providers and treatments sought):

- https://atriumhealth.org/search-atrium-health#q=vision&sort=relevancy
- https://atriumhealth.org/search-atrium-health#q=muscular%20dystrophy&sort=relevancy
- https://atriumhealth.org/search-atrium-health#q=support%20groups&sort=relevancy
- https://atriumhealth.org/search-atrium-health#q=spinal%20surgery&sort=relevancy
- https://atriumhealth.org/search-atrium-health#q=er&sort=relevancy
- https://atriumhealth.org/locations/emergency-departments
- https://atriumhealth.org/find-a-doctor

85. Contemporaneously with the interception and transmission of the contents of Plaintiff J.S.'s communications regarding her condition on https://www.atriumhealth.org/,

Defendant also disclosed to Meta Plaintiff J.S.'s unique personal identifiers, including but not limited to, her Facebook ID and IP address.

86. During the relevant time period, when the Defendant's Pixels were present, Plaintiff J.S. also utilized Defendant's Patient Portal to review her medical records such as her visit summaries, doctor's notes and her test results.

87. Upon information and good faith belief, Defendant intercepted at least the following communications about Plaintiff J.S.'s patient status, via the following URLs or substantially similar URLs were sent to Meta via the Pixel, indicating that Plaintiff J.S. is a patient of Defendant who is about to use the patient portal:

- https://my.atriumhealth.org/myatriumhealth/authentication/login

88. Plaintiff J.S. reasonably expected that her communications with Defendant via the Web Properties were confidential, solely between herself and Defendant, and that such communications would not be transmitted to or intercepted by a third party.

89. Plaintiff J.S. provided her Private Information to Defendant and trusted that the information would be safeguarded according to Defendant's policies and state and federal law.

90. As described herein, Defendant worked along with Facebook to intercept Plaintiff J.S.'s communications, including those that contained their Private Information.

91. Defendant willfully facilitated these interceptions without Plaintiff J.S.'s knowledge, consent or express written authorization.

92. Defendant transmitted to Facebook Plaintiff J.S.'s Facebook ID, computer IP address and sensitive health information such as her medical symptoms, conditions, treatments sought, physician selected, button/menu selections and/or content typed into free text boxes.

93. By doing so without her consent, Defendant breached Plaintiff J.S.'s privacy and unlawfully disclosed their Private Information.

94. Defendant did not inform Plaintiff J.S. that it had shared her Private Information with Facebook.

FACTUAL BACKGROUND

A. The Irresponsible Use of Invisible Tracking Codes by Healthcare Providers to Send Meta People's Data for its Advertising Business.

95. Meta operates the world's largest social media company whose revenue is derived almost entirely from selling targeted advertising.

96. The Meta Pixel and other third-party tracking tools also collect and transmit information from Defendant that identifies a Facebook user's status as a patient and other health information that is protected by federal and state law. This occurs through tools that Facebook encourages its healthcare Partners to use, including to upload patient lists to Facebook for use in its advertising systems.

97. Meta associates the information it obtains via the Meta Pixel with other information regarding the User, using personal identifiers that are transmitted concurrently with other information the Pixel is configured to collect.

98. For Facebook account holders, these identifiers include the "c_user" cookie IDs, which allow Meta to link data to a particular Facebook account. For both Facebook account holders and users who do not have a Facebook account, these identifiers also include cookies that Meta ties to their browser.

99. Realizing the value of having direct access to millions of consumers, in 2007, Facebook began monetizing its platform by launching "Facebook Ads," proclaiming it to be a

"completely new way of advertising online" that would allow "advertisers to deliver more tailored and relevant ads."[8]

100. One of its most powerful advertising tools is Meta Pixel, formerly known as Facebook Pixel, which launched in 2015.

101. Ad targeting has been extremely successful due, in large part, to Facebook's ability to target people at a granular level. "Among many possible target audiences, Facebook offers advertisers, [for example,] 1.5 million people 'whose activity on Facebook suggests that they're more likely to engage with/distribute liberal political content' and nearly seven million Facebook users who 'prefer high-value goods in Mexico.'"[9]

102. The Meta Pixel is a free and publicly available "piece of code" that third-party web developers can install on their website to "measure, optimize and build audiences for … ad campaigns."[10]

103. Meta describes the Pixel as "a snippet of JavaScript code" that "relies on Facebook cookies, which enable [Facebook] to match … website visitors to their respective Facebook user accounts.[11]

---

[8] *Facebook Unveils Facebook Ads*, META (November 6, 2007), https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/.

[9] Natasha Singer, *What You Don't Know about How Facebook Uses Your Data* (April 11, 2018), https://www.nytimes.com/2018/04/11/technology/facebook-privacy-hearings.html.

[10] *Meta Pixel* (2023), https://www.facebook.com/business/tools/meta-pixel.

[11] *Meta Pixel* (2023), https://developers.facebook.com/docs/meta-pixel/.

104. Meta pushes advertisers to install the Meta Pixel. Meta tells advertisers the Pixel "can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart."[12]

105. Meta tells advertisers that the Meta Pixel will improve their Facebook advertising, including by allowing them to:

a. "optimize the delivery of your ads" and "[e]nsure your ads reach the people most likely to take action;" and

b. "create Custom Audiences from website visitors" and create "[d]ynamic ads [to] help you automatically show website visitors the products they viewed on your website—or related ones."[13]

106. Meta explains that the Pixel "log[s] when someone takes an action on your website" such as "adding an item to their shopping cart or making a purchase," and the user's subsequent action:

Once you've set up the Meta Pixel, the Pixel will log when someone takes an action on your website. Examples of actions include adding an item to their shopping cart or making a purchase. The Meta Pixel receives these actions, or events, which you can view on your Meta Pixel page in Events Manager. From there, you'll be able to see the actions that your customers take. You'll also have options to reach those customers again through future Facebook ads.

[12] *Meta Pixel* (2023), https://www.facebook.com/business/tools/meta-pixel.

[13] *Id.*

107. The Meta Pixel is customizable and web developers can choose the actions the Pixel will track and measure on a particular webpage.

108. Meta advises web developers to place the Pixel early in the source code[14] for any given webpage or website to ensure that visitors will be tracked before they leave the webpage or website.[15]

109. Meta's "Health" division is dedicated to marketing to and servicing Meta's healthcare "Partners." Meta defines its "Partners" to include businesses that use Meta's products, including the Meta Pixel or Meta Audience Network tools to advertise, market, or support their products and services.

110. Meta works with hundreds of Meta healthcare Partners, using Meta Collection Tools to learn about visitors to their websites and leverage that information to sell targeted advertising based on patients' online behavior. Meta's healthcare Partners also use Meta's other ad targeting tools, including tools that involve uploading patient lists to Meta.

111. Healthcare providers like Defendant encourage Plaintiffs and Class Members to access and use various digital tools via its Web Properties to, among other things, receive healthcare services, in order to gain additional insights into its Users, improve its return on marketing dollars and, ultimately, increase its revenue.

---

[14] Source code is a collection of instructions (readable by humans) that programmers write using computer programming languages such as JavaScript, PHP, and Python. When the programmer writes a set or line of source code, it is implemented into an application, website, or another computer program. Then, that code can provide instructions to the website on how to function. *What is Source Code & Why Is It Important?* (July 19, 2023), https://blog.hubspot.com/website/what-is-source-code (last visited Apr. 4, 2024).

[15] *Meta Pixel: Get Started* (2023), *https://developers.facebook.com/docs/meta- pixel/get-started.*

112. In exchange for installing the Pixels, Facebook provided Defendant with analytics about the advertisements it has placed as well as tools to target people who have visited its Web Properties.

113. Upon information and belief, Defendant and other companies utilized Plaintiffs' and Class Members' sensitive information and data collected by the Meta Pixels on Defendant's Web Properties in order to advertise to these individuals later on Meta's social platforms.

114. If a healthcare provider, such as Defendant, installs the Meta Pixel code as Meta recommends, patients' actions on the provider's website are contemporaneously redirected to Meta.

115. For example, when a patient clicks a button to register for, or logs into or out of, a "secure" patient portal, Meta's source code commands the patient's computing device to send the content of the patient's communication to Meta while the patient is communicating with their healthcare provider.

116. In other words, by design, Meta receives the content of a patient's portal log in communication immediately when the patient clicks the log-in button—even before the healthcare provider receives it. [16]

[16] At the time of filing this complaint, Plaintiffs are unable to determine whether Pixels were embedded inside Defendant's MyChart Portal. However, given Defendant's use of the Meta Pixel on other pages of the Website *including the log-in page for its patient Portal*, Plaintiffs reasonably believe and, therefore, aver that Defendant used the Pixels to track information on its entire digital platform, including inside its MyChart Portal. *See also*, Todd Feathers, *et al.*, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, THE MARKUP (June 16, 2022) (listing examples of hospitals that used third party trackers inside password-protected patient portals), https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

117. Thus, the Meta "pixel allows Facebook to be a silent third-party watching whatever you're doing,"[17] which in this case included the content of Defendant's patients' communications with its Web Properties, including their PHI.

118. For Facebook, the Pixel acts as a conduit of information, sending the information it collects to Facebook through scripts running in the User's internet browser, via data packets labeled with PII, including the User's IP address, the Facebook c_user cookie and third-party cookies allowing Facebook to link the data collected by Meta Pixel to the specific Facebook user.[18]

119. A recent investigation by The Markup revealed that the Meta Pixel was installed inside password-protected patient portals of at least seven U.S. health systems, giving Facebook access to even more patient communications with their providers.[19]

120. David Holtzman, a health privacy consultant was "deeply troubled" by the results of The Markup's investigation and indicated "it is quite likely a HIPAA violation" by the hospitals, such as Defendant.[20]

121. Facebook's access to use even only some of these data points—such as just a "descriptive" webpage URL—is problematic. As Laura Lazaro Cabrera, a legal officer at Privacy

---

[17] Jefferson Graham, *Facebook spies on us but not by recording our calls. Here's how the social network knows everything* (Apr. 4, 2020), https://www.usatoday.com/story/tech/2020/03/04/facebook-not-recording-our-calls-but-has-other-ways-snoop/4795519002/.

[18] The Facebook Cookie is a workaround to recent cookie-blocking techniques, including one developed by Apple, Inc., to track users. *See* Maciej Zawadziński & Michal Wlosik, *What Facebook's First-Party Cookie Means for AdTech* (June 8, 2022), https://clearcode.cc/blog/facebook-first-party-cookie-adtech/.

[19] *See* Feathers, *supra,* note 16.

[20] *Id.*

International, explained: "Think about what you can learn from a URL that says something about scheduling an abortion' . . . 'Facebook is in the business of developing algorithms. They know what sorts of information can act as a proxy for personal data."[21]

122. The collection and use of this data raises serious concerns about user privacy and the potential misuse of personal information. For example, when Users browse Defendant's Web Properties, every step of their activity is tracked and monitored. By analyzing this data using algorithms and machine learning techniques, Facebook (and other entities tracking this information) can learn a chilling level of detail about Users' medical conditions, behavioral patterns, preferences, and interests.

123. This data can be used not only to provide personalized and targeted content and advertising, but also for more nefarious purposes, such as tracking and surveillance. Moreover, the misuse of this data could potentially lead to the spread of false or misleading information, which could have serious consequences, particularly in the case of health-related information.

124. As pointed out by the Office for Civil Rights (OCR) at the U.S. Department of Health and Human Services (HHS), impermissible disclosures of such data in the healthcare context "may result in identity theft, financial loss, discrimination, stigma, mental anguish, or other serious negative consequences to the reputation, health, or physical safety of the individual or to

[21] Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics Are Collecting Highly Sensitive Info on Would-Be Patients*, THE MARKUP (Sept. 25, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients.

others identified in the individual's PHI…. This tracking information could also be misused to promote misinformation, identity theft, stalking, and harassment."[22]

125. Unfortunately, several recent reports detail the widespread use of third-party tracking technologies on hospitals', health care providers' and telehealth companies' digital properties to surreptitiously capture and to disclose their Users' Private Information.[23] Estimates are that over 664 hospital systems and providers utilize some form of tracking technology on their digital properties.[24]

B. Defendant Disclosed Patient Healthcare Information, Including Patient Status, in Violation of the HIPAA Privacy Rule.

126. Healthcare entities collecting and disclosing Users' Private Information face significant legal exposure under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), which applies specifically to healthcare providers, health insurance providers and healthcare data clearinghouses.[25]

---

[22] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (last visited Mar. 12, 2024).

[23] The Markup reported that 33 of the largest 100 hospital systems in the country utilized the Meta Pixel to send Facebook a packet of data whenever a person clicked a button to schedule a doctor's appointment. Todd Feathers, *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, *supra*, note 16.

[24] Dave Muoio & Annie Burky, *Advocate Aurora, WakeMed get served class action over Meta's alleged patient data mining,* FIERCE HEALTHCARE (November 4, 2022), https://www.fiercehealthcare.com/health-tech/report-third-top-hospitals-websites-collecting-patient-data-facebook.

[25] *Health Information Privacy* (Mar. 31, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

127. The HIPAA privacy rule sets forth policies to protect all individually identifiable health information ("IIHI") that is held or transmitted.[26] This is information that can be used to identify, contact, or locate a single person or can be used with other sources to identify a single individual.

128. Plaintiffs' IIHI captured by the Pixel and sent to Meta included their unique personal identifiers such as their Facebook ID, IP address, device identifiers and browser "fingerprints."

129. Defendant further violated the HIPAA Privacy Rule, among other statutory and common laws, because Plaintiffs' PHI concerning their specific medical conditions (such as Plaintiff J.R.'s pulmonology visits, Plaintiff's J.S.'s vision visits) was disclosed to Meta by the Pixel and other third-party trackers embedded by Defendant on its Web Properties.

130. HIPAA also protects against revealing an individual's status as a patient of a healthcare provider.[27]

131. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1).

132. Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

---

[26] The HIPAA Privacy Rule protects all electronically protected health information a covered entity like Defendant "created, received, maintained, or transmitted" in electronic form. *See* 45 C.F.R. § 160.103.

[27] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule*, https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html (last visited Apr. 4, 2024).

133. Defendant unlawfully revealed Plaintiffs' and Class Members' patient status to Facebook and likely other unauthorized third parties in violation of HIPAA when the Meta Pixel captured and disclosed Plaintiffs' and Class Members' activity on patient-dedicated webpages of the Web Properties, such as Patient Financial Services, Patient Education Resources, Schedule an Appointment, and the Patient Portal.

C. HIPAA's Protections Do Not Exclude Internet Marketing.

134. The Office for Civil Rights at HHS has made clear, in a recently updated bulletin entitled *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, that the transmission of such protected information violates HIPAA's Privacy Rule:

> Regulated entities [those to which HIPAA applies] are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules. ***For example, disclosures of PHI to tracking technology vendors for marketing purposes, without individuals' HIPAA-compliant authorizations, would constitute impermissible disclosures.***[28]

135. Here, Defendant provided patient information to third parties in violation of the Privacy Rule. HHS has repeatedly instructed for years that patient status is protected by the HIPAA Privacy Rule:

> a. "The sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);
>
> b. "A covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002); and

[28] *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates,* https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (emphasis added) (updated March 18, 2024) (last visited April 4, 2024).

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013).

136. In addition, the Office for Civil Rights at HHS' Bulletin expressly provides that "**[r]egulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules.**"[29]

137. Tracking technology vendors like Facebook and Google are considered business associates under HIPAA where, as here, they provide services to Defendant and receive and maintain PHI.

> Furthermore, tracking technology vendors are business associates if they create, receive, maintain, or transmit PHI on behalf of a regulated entity for a covered function (*e.g.* health care operations) or provide certain services to or for a covered entity (or another business associate) that involve the disclosure of PHI. In these circumstances, regulated entities must ensure that the disclosures made to such vendors are permitted by the Privacy Rule and enter into a business associate agreement (BAA) with these tracking technology vendors to ensure that PHI is protected in accordance with the HIPAA Rules. For example, if an individual makes an appointment through the website of a covered health clinic for health services and that website uses third party tracking technologies, then the website might automatically transmit information regarding the appointment and the individual's IP address to a tracking technology vendor. In this case, the tracking technology vendor is a business associate and a BAA is required.[30]

138. The Bulletin further explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information (like an IP address)

[29] *Id.*
[30] *Id.*

even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> **Some regulated entities may be disclosing a variety of information to tracking technology vendors through tracking technologies placed on the regulated entity's website or mobile app, such as information that the individual types or selects when they use regulated entities' websites or mobile apps**. The information disclosed might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, device IDs, or any unique identifying code.
>
> ---
>
> IIHI collected on a regulated entity's website or mobile app generally is PHI, **even if the individual does not have an existing relationship with the regulated entity** and even if the IIHI, such as in some circumstances IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services.[31]

139. HIPAA applies to Defendant's webpages with tracking technologies even outside the patient portal:

> Tracking on unauthenticated webpages
>
> Regulated entities may also have unauthenticated webpages, which are webpages that do not require users to log in before they are able to access the webpage, such as a webpage with general information about the regulated entity like their location, visiting hours, employment opportunities, or their policies and procedures… **in some cases, tracking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors**. Regulated entities are required to "[e]nsure the confidentiality, integrity, and availability of all electronic PHI the [regulated entity] creates, receives, maintains, or transmits." Thus, regulated entities that are

[31] *Id.* (emphasis added).

> considering the use of online tracking technologies should consider whether any PHI will be transmitted to a tracking technology vendor, and take appropriate steps consistent with the HIPAA Rules.[32]

140. HHS explained that, if the online tracking technologies on the webpages have access to information that relates to an individual's past, present, or future health, health care, or payment for health care, that is a disclosure of PHI, for example:

> [I]f an individual were looking at a hospital's webpage **listing its oncology services** to seek a second opinion on treatment options for their brain tumor, **the collection and transmission of the individual's IP address, geographic location, or other identifying information showing their visit to that webpage is a disclosure of PHI** to the extent that the information is both identifiable and related to the individual's health or future health care.

141. HHS also explained in the Bulletin that tracking technologies on health care providers' patient portals "generally have access to PHI" and may access diagnoses and treatment information, in addition to other sensitive data:

> Tracking on user-authenticated webpages
>
> Regulated entities may have user-authenticated webpages, which require a user to log in before they are able to access the webpage, such as a patient or health plan beneficiary portal or a telehealth platform. **Tracking technologies on a regulated entity's user-authenticated webpages generally have access to PHI.** Such PHI may include, for example, an individual's IP address, medical record number, home or email addresses, dates of appointments, or other identifying information that the individual may provide when interacting with the webpage. Tracking technologies within user-authenticated webpages may even have access to an individual's diagnosis and treatment information, prescription information, billing information, or other information within the portal. Therefore, a regulated entity must configure any user-authenticated webpages that include tracking technologies to allow such technologies to only use and disclose PHI in compliance with the HIPAA Privacy Rule and must ensure that the electronic protected

[32] *Id.* (emphasis added).

> health information (ePHI) collected through its website is protected and secured in accordance with the HIPAA Security Rule.[33]

142. The Bulletin is not a pronouncement of new law, but instead a reminder to covered entities and business associates of their longstanding obligations under existing guidance.

143. The Bulletin notes that "it has always been true that regulated entities may not impermissibly disclose PHI to tracking technology vendors," then explains how online tracking technologies violate the same HIPAA rules that have existed for decades.[34]

144. In other words, HHS has expressly stated that Defendant has violated HIPAA Rules by implementing the Meta Pixel.

145. As a result, a healthcare provider like Defendant may not disclose PHI to a tracking technology vendor, like Meta, unless it has properly notified its Website Users and entered into a business associate agreement with the vendor in question.

146. Defendant disclosed Plaintiffs' and Class Members' PHI without their consent and without a business associate agreement with Meta.

---

[33] *Id.* (emphasis added).

[34] *Id.* (citing, *e.g.*, Modifications of the HIPAA [Rules], Final Rule," 78 FR 5566, 5598, a rulemaking notice from January 25, 2013, which stated: "[P]rotected health information … may not necessarily include diagnosis-specific information, such as information about the treatment of an individual, and may be limited to demographic or other information not indicative of the type of health care services provided to an individual. If the information is tied to a covered entity, then it is protected health information by definition since it is indicative that the individual received health care services or benefits from the covered entity, and therefore it must be protected … in accordance with the HIPAA rules." at n. 22).

D. Defendant Transmitted a Broad Spectrum of Plaintiffs' & Class Members' Identifiable Health Information to Meta via the Meta Tracking Tools.

147. Every website is comprised of "Markup" and "Source Code." Markup consists of the pages, images, words, buttons, and other features that appear on the patient's screen as they navigate Defendant's Web Properties.

148. Source Code is a set of instructions that commands the website visitor's browser to take certain actions when the web page first loads or when a specified event triggers the code. Source Code is designed to be readable by humans and formatted in a way that developers and other users can understand.

149. In addition to controlling a website's Markup, Source Code executes a host of other programmatic instructions including the ability to command a website user's browser to send data transmissions to third parties like Facebook, via the Meta Pixel.[35]

150. Defendant's Pixel, embedded in its JavaScript Source Code on the Web Properties, manipulates a User's browser by secretly instructing it to duplicate a User's communications (HTTP Requests) and sending those communications to Facebook.

151. This occurs because the Pixel is programmed to automatically track and transmit Users' communications, and this occurs contemporaneously, invisibly, and without the Users' knowledge.

152. Defendant's Source Code essentially commands a patient's browser to re-direct their actions on the Web Properties (characterized as "Event Data" by the Pixel), which contain PHI, through the HTTPS protocol to Meta at a Meta "endpoint," i.e., a URL at a domain controlled by Meta that exists for the purpose of acquiring such information.

[35] These Pixels or web bugs are tiny image files that are invisible to website users. They are purposefully designed in this manner, or camouflaged, so that users remain unaware of them.

153. The information Defendant sends to Meta from its use of the Meta Pixel and other tracking tools includes, but is not limited to, the following:

a. The exact search terms entered by a User on the Website, including searches for the User's medical symptoms and conditions, specific medical providers and their specialty, and treatments sought;

b. descriptive URLs that describe the categories of the Website, categories that describe the current section of the Website, and the referrer URL that caused navigation to the current page;

c. the communications a User exchanges through Defendant's Web Properties by clicking and viewing webpages, including communications about providers and specialists, conditions, and treatments, along with the timing of those communications, including, upon information and good faith belief, whether they are made while a User is still logged in to the Patient Portal or around the same time that the User has scheduled an appointment, called the medical provider, or logged in or out of the Patient Portal;

d. when a User sets up or schedules an appointment;

e. information that a User clicks on in an appointment form;

f. when a User clicks a button to call the provider from a mobile device directly from Defendant's Website;

g. when a User clicks to register for the Patient Portal, clicks to log into the Portal, and/or accesses other patient-dedicated web pages; and

h. the same or substantially similar communications that patients exchange with health insurance companies, pharmacies, and prescription drug companies.

154. Thus, Defendant is, in essence, handing patients a tapped device and once one of its webpages is loaded into the User's browser, the software-based wiretap is quietly waiting for private communications on the webpage to trigger the tap, which intercepts those communications—intended only for Defendant—and transmits those communications to unauthorized third parties such as Facebook.

155. For example, when a patient visits www.atriumhealth.org and enters "heart disease," "diabetes" or "stroke rehabilitation" into the search bar, their browser automatically sends an HTTP request to Defendant's web server. Defendant's web server automatically returns an HTTP response, which loads the Markup for that particular webpage.

156. The patient visiting this particular web page only sees the Markup, not the Defendant's source code or underlying HTTP Requests and Responses.

157. In reality, Defendant's Source Code and underlying HTTP Requests and Responses share the patient's personal information with Facebook, including the fact that a User was looking for treatment for their heart disease, diabetes, or stroke diagnosis — along with the User's unique personal identifiers.

Figure 1: An example of a HTTP communication session sent by the Pixel from the User's device to Facebook that reveals the User's search for "cancer"

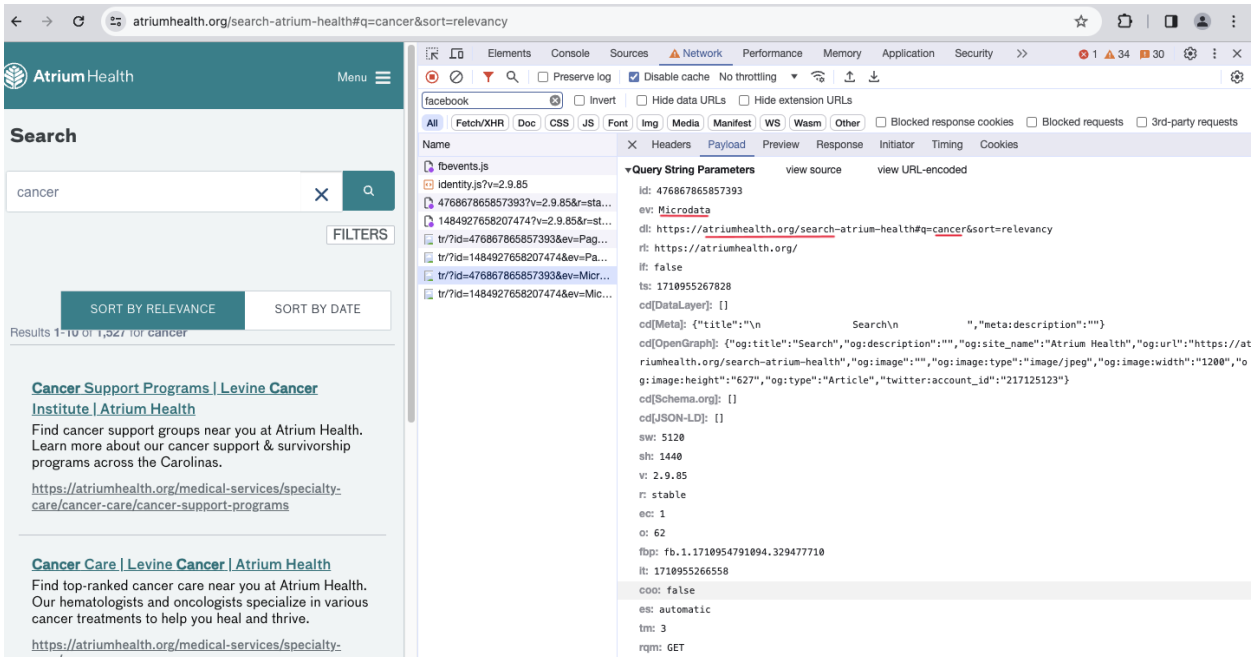
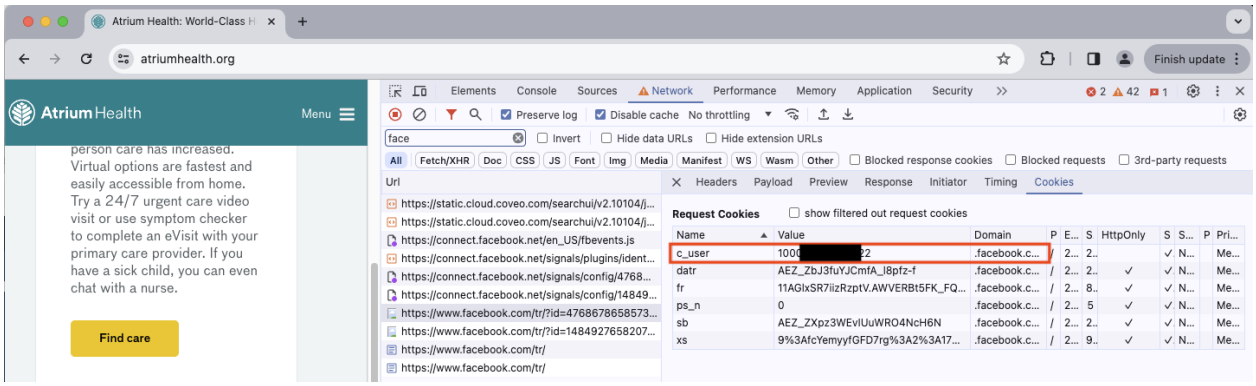


Figure 2. An easier-to-read representation of the User's c_user ID sent to Facebook when a User enters a new page of Defendant's website.



158. In recent months, following a wave of negative press and litigation against other healthcare companies for the same unlawful activities, Defendant has removed the Meta Pixel from its Web Properties and has re-configured its source code.

159. However, because of the way Defendant's source code operated with the embedded Meta Pixel, when Plaintiff J.R. used the search bar on https://www.atriumhealth.org to look for medical treatments for pulmonologists, their exact search terms (including "pulmonology" and other similar terms) were transmitted by Defendant's Pixel to Meta, disclosing their specific medical conditions.

160. Similarly, when Plaintiff J.S. used the search bar on https://www.atriumhealth.org to look up their medical conditions and potential treatments for it (including "vision", "eye doctor", and other similar terms) were transmitted by Defendant's Pixel to Meta, disclosing their specific medical conditions.

161. When Plaintiffs and Class Members clicked on Defendant's "Medical Services" tab, it took them to the list of services offered by Defendant to Users in need of various medical treatments. On those pages the User can further narrow their search results by services offered by Defendant.

162. The User's selections and filters are transmitted to Facebook via the Meta Pixels, even if they contain the User's treatment, procedures, medical conditions, or related queries,

without alerting the User, and the images below confirm that the communications Defendant sends to Facebook contain the User's Private Information and personal identifiers, including but not limited to their IP address, Facebook ID, and datr and fr cookies, along with the search filters the User selected.

163. For example, a diabetes patient in search for diabetes services can search for various diabetes treatment options and information, from "endocrinology clinic" and "diabetes prevention" to resources intended to help patients.[36]

164. From the moment the patient begins searching for diabetes treatment their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the User's unique personal identifiers.

165. The transmission identifies the User as a patient: (i) seeking medical care from Defendant via www.atriumhealth.org; (ii) who has diabetes; and (iii) who is searching for diabetes services.

166. Similarly, a patient who has experienced a stroke can search for post-stroke treatments, including rehabilitation services.

167. From the moment the patient begins searching for post-stroke treatment their selections or search parameters are automatically transmitted by the Pixel to Facebook along with the User's unique personal identifiers.

168. The transmission identifies the User as a patient: (i) seeking medical care from Defendant via www.atriumhealth.org; (ii) who has had a stroke; and (iii) who is searching for stroke rehabilitation services.

[36] *See Atrium Health Endocrinology,* ATRIUM HEALTH, https://atriumhealth.org/locations/detail/atrium-health-endocrinology-union-west.

169. If the patient chooses to click the phone number for Defendant's flagship hospital, Carolinas Medical Center, that action is shared with Meta as well, via a "SubscribedButtonClick" event which captures the phone number of the clinic accessed by the patient.

170. As described above, if the patient selects other services, those search parameters are also automatically transmitted to Facebook by Defendant's Pixel, along with the patient's personal identifiers.

171. For example, after Plaintiff J.S.'s vision issues, she looked up information and appointments through Defendant's website.

172. This information would have been disclosed to Facebook (and likely other unauthorized third parties at least in the form of a descriptive URL, https://atriumhealth.org/medical-services/specialty-care/rehabilitation/spinal-cord-injury, along with Plaintiff J.S.'s unique personal identifiers including their Facebook ID and IP address.

173. Defendant would have also shared the fact that several times in the past five years Plaintiff J.S. was looking up information on Muscular Dystrophy to help care for her mother, who has been diagnosed with that condition.

174. For Plaintiff J.R., Defendant would have disclosed that starting in May 2020 she was looking up pulmonologists, including but not limited to sharing the descriptive URL https://atriumhealth.org/locations/detail/atrium-health-pulmonology-university-city that she visited on Defendant's Website.

E. Defendant's Web Properties Sent Plaintiffs' and Class Members' PHI to Facebook Along with Unique Personal Identifiers.

175. As described herein, Defendant's Meta Pixel (and other third-party trackers) sent sensitive Private Information to Facebook, including but not limited to Plaintiffs' and Class Members': (i) status as medical patients; (ii) health conditions; (iii) sought treatments or therapies;

(iv) terms and phrases entered into Defendant's search bar; (v) sought providers and their specialties; (vi) selected locations or facilities for treatment and (vii) web pages viewed.

176. Importantly, the Private Information Defendant's Pixel sent to Facebook was sent alongside Plaintiffs' and Class Members' personal identifiers, including patients' IP address and cookie values such as their unique Facebook ID, thereby allowing individual patients' communications with Defendant, and the Private Information contained in those communications, to be linked to their unique Facebook accounts.

177. Through the source code deployed by Defendant, the cookies that it uses to help Facebook identify patients include but are not necessarily limited to cookies named: "c_user," "datr," "fr," and "fbp."

178. A User's FID is linked to their Facebook profile, which generally contains a wide range of demographics and other information about the User, including pictures, personal interests, work history, relationship status, and other details. Because the User's Facebook Profile ID uniquely identifies an individual's Facebook account, Facebook—or any ordinary person—can easily use the Facebook Profile ID to quickly and easily locate, access, and view the User's corresponding Facebook profile.

179. The "datr" cookie identifies the patient's specific web browser from which the patient is sending the communication. It is an identifier that is unique to the patient's specific web browser and is therefore a means of identification for Facebook users.

180. The "fr" cookie is a Facebook identifier that is an encrypted combination of the c_user and datr cookies.[37] Facebook, at a minimum, uses the fr cookie to identify Users.[38]

181. At each stage, Defendant also utilized the _fbp cookie, which attaches to a browser as a first-party cookie, and which Facebook uses to identify a browser and a User:[39]

182. The fr cookie expires after ninety (90) days unless the User's browser logs back into Facebook.[40] If that happens, the time resets, and another ninety (90) days begins to accrue.

183. The _fbp cookie expires after ninety (90) days unless the User's browser accesses the same website.[41] If that happens, the time resets, and another ninety (90) days begins to accrue.

184. The Facebook Meta Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—i.e., Defendant.[42]

185. A third-party cookie is "created by a website with a domain name other than the one the user is currently visiting"—i.e., Facebook.[43]

---

[37] *See* Gunes Acar et al., *Facebook Tracking Through Social Plug-ins: Technical Report prepared for the Belgian Privacy Commission* 16 (March 27, 2015), https://securehomes.esat.kuleuven.be/~gacar/fb_tracking/fb_pluginsv1.0.pdf.

[38] *Cookies Policy*, META, https://www.facebook.com/policy/cookies/ (last visited Apr. 4, 2024).

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] This is confirmable by using developer tools to inspect a website's cookies and track network activity.

[43] This is confirmable by tracking network activity.

186. The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

187. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to FIDs and corresponding Facebook profiles.

188. As shown in the figures above, Defendant sent these identifiers with the event data.

189. Plaintiffs never consented, agreed, authorized, or otherwise permitted Defendant to disclose their Private Information, nor did they authorize any assistance with intercepting their communications.

190. Plaintiffs were never provided with any written notice that Defendant disclosed its Website Users' Private Information nor were they provided any means of opting out of such disclosures.

191. Despite this, Defendant knowingly and intentionally disclosed Plaintiffs' Private Information to Facebook.

F. Defendant Violates Its Promises to Users and Patients to Protect Their Confidentiality.

192. Beyond Defendant's legal obligations to protect the confidentiality of individuals' Private Information, Defendant's privacy policies and online representations affirmatively and unequivocally state that any personal information provided to Defendant will remain secure and protected.[44]

[44] *Privacy Policy*, ATRIUM HEALTH, https://atriumhealth.org/for-patients-visitors/privacy/english (last visited Apr. 4, 2024).

193. Further, Defendant represents to Users that it will only disclose Private Information provided to them under certain circumstances, none of which apply here.[45] Defendant's privacy policies do not permit Defendant to use and disclose Plaintiffs' and Class Members' Private Information for marketing purposes.

194. In fact, Defendant acknowledges in its Notice of Privacy Practices that "we do not sell your information or get paid by vendors to communicate with you without your written authorization."[46]

195. Moreover, Defendant represents that it will disclose Users' PHI when required to in limited circumstances. Defendant represents that it may transfer or share User's PHI with "other people and companies, known as business associates, to help us perform services and manage our operations," or "as required by local, state or federal law."[47]

196. Further, Defendant's Privacy Policy represents: "We understand that your health information is personal and we are committed to protecting your privacy… We are required by law to: Maintain the privacy of your health information as outlined in this Notice"[48]

197. Upon information and belief, none of these circumstances listed above apply here.

198. In its separate Online Privacy Policy, Defendant also separately acknowledges that, "we will not sell your Personal Information without your express permission."[49]

---

[45] *See id*.

[46] *See id.*

[47] *See id.*

[48] *See id.*

[49] *Online Privacy Policy*, ATRIUM HEALTH, https://atriumhealth.org/for-patients-visitors/online-privacy-policy.

199. Defendant failed to issue a notice that Plaintiffs' and Class Members' Private Information had been impermissibly disclosed to an unauthorized third party. In fact, Defendant never disclosed to Plaintiffs or Class Members that it shared their sensitive and confidential communications, data, and Private Information with Meta and other unauthorized third parties.[50]

200. Through Plaintiffs' payment for healthcare services with Defendant for many years, the terms of Defendant's privacy policies necessarily formed essential terms of its contracts for those services. Indeed, Defendant required Plaintiffs to sign acknowledgments of receipt of Defendant's Notice of Privacy Practices prior to receiving any healthcare services, and Plaintiffs understood that as part of their bargain for healthcare services with Defendant, Defendant would keep its promises of confidentiality regarding their sensitive PHI, however it was to be received by Defendant.

201. Defendant has unequivocally failed to adhere to a single promise to safeguard Private Information of its Users. Defendant has made these privacy policies and commitments available on its websites. Defendant includes these privacy policies and commitments to maintain the confidentiality of its Users' sensitive information as terms of its contracts with those Users, including contracts entered with Plaintiffs and the Class Members. In these contract terms and other representations to Plaintiffs and Class Members and the public, Defendant promised to take

[50] In contrast to Defendant, in recent months several medical providers which have installed the Meta Pixel on its Web Properties have provided its patients with notices of data breaches caused by the Pixel transmitting PHI to third parties. *See*, *e.g.*, *Cerebral, Inc. Notice of HIPAA Privacy Breach*, https://cerebral.com/static/hippa_privacy_breach-4000c6eb21449c2ecd8bd13706750cc2.pdf; Annie Burky, *Advocate Aurora says 3M patients' health data possibly exposed through tracking technologies,* FIERCE HEALTHCARE (October 20, 2022), https://www.fiercehealthcare.com/health-tech/advocate-aurora-health-data-breach-revealed-pixels-protected-health-information-3; *Novant Health Notifies Patients of Potential Data Privacy Incident*, PR NEWSWIRE (August 19, 2022), https://www.prnewswire.com/news-releases/novant-health-notifies-patients-of-potential-data-privacy-incident-301609387.html.

specific measures to protect Plaintiffs' and Class Members' Private Information, consistent with industry standards and independent from federal and state law. However, it failed to do so.

202. Even non-Facebook users can be individually identified via the information gathered on the Digital Platforms, like an IP address or personal device identifying information. This is precisely the type of information for which HIPAA requires the use of de-identification techniques to protect patient privacy.[51]

203. In fact, in an action currently pending against Facebook related to use of its Pixel on healthcare provider web properties, Facebook explicitly stated it requires Pixel users to "post a prominent notice on every page where the Pixel is embedded and to link from that notice to information about exactly how the Pixel works and what is being collected through it, so it is not invisible."[52] Defendant did not post such a notice.

204. Facebook further stated that "most providers [...] will not be sending [patient information] to Meta because it violates Meta's contracts for them to be doing that."[53]

205. Despite a lack of disclosure, Defendant allowed third parties to "listen in" on patients' confidential communications and to intercept and use for advertising purposes the very information they promised to keep private, in order to bolster their profits.

---

[51] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule, supra,* note 27.

[52] *See* Transcript of the argument on Plaintiff's Motion for Preliminary Injunction in *In re Meta Pixel Healthcare Litig.*, Case No. CV-22-03580-WHO (N.D. Cal. Nov. 9, 2022) (Hon. J. Orrick), at 19:12-18; *see also In re Meta Pixel Healthcare Litig*., 2022 WL 17869218 (N.D. Cal. Dec 22, 2022).

[53] *Id.* at 7:20-8:11.

G. Plaintiffs and Class Members Reasonably Believed That Their Confidential Medical Information Would Not Be Shared with Third Parties.

206. Plaintiffs and Class Members were aware of Defendant's duty of confidentiality when they sought medical services from Defendant.

207. Indeed, at all times when Plaintiffs and Class Members provided their Private Information to Defendant, they each had a reasonable expectation that the information would remain confidential and that Defendant would not share the Private Information with third parties for a commercial purpose, unrelated to patient care.

208. Personal data privacy and obtaining consent to share Private Information are material to Plaintiffs and Class Members.

209. Plaintiffs and Class Members relied to their detriment on Defendant's uniform representations and omissions regarding protection privacy, limited uses, and lack of sharing of their Private Information.

210. Now that their sensitive personal and medical information is in possession of third parties, Plaintiffs and Class Members face a constant threat of continued harm including bombardment of targeted advertisements based on the unauthorized disclosure of their personal data. Collection and sharing of such sensitive information without consent or notice poses a great threat to individuals by subjecting them to the never-ending threat of identity theft, fraud, phishing scams, and harassment.

H. Plaintiffs and Class Members Have No Way of Determining Widespread Usage of Invisible Pixels.

211. Plaintiffs and Class Members did not realize that tracking Pixels exist because they are invisibly embedded within Defendant's web pages that Users might interact with.[54] Patients and Users of Defendant's Web Properties do not receive any alerts during their uses of Defendant's Web Properties stating that Defendant tracks and shares sensitive medical data with Facebook, allowing Facebook and other third parties to subsequently target all Users of Defendant's website for marketing purposes.

212. Plaintiffs and Class Members trusted Defendant's Web Properties when inputting sensitive and valuable Private Information. Had Defendant disclosed to Plaintiffs and Class Members that every click, every search, and every input of sensitive information was being tracked, recorded, collected, and disclosed to third parties, Plaintiffs and Class Members would not have trusted Defendant's Web Properties to input such sensitive information.

213. Defendant knew or should have known that Plaintiffs and Class Members would reasonably rely on and trust Defendant's promises regarding the tracking privacy and uses of their Private Information. Furthermore, any person visiting a health website has a reasonable understanding that medical providers must adhere to strict confidentiality protocols and are bound not to share any medical information without their consent.

214. By collecting and sharing Users' Private Information with Facebook and other unauthorized third parties, Defendant caused harm to Plaintiffs, Class Members, and all affected individuals.

215. Furthermore, once Private Information is shared with Facebook, such information may not be effectively removed, even though it includes personal and private information.

---

[54] *See, e.g.*, FTC Office of Technology, *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FED. TRADE COMM'N (March 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

216. Plaintiffs fell victim to Defendant's unlawful collection and sharing of their sensitive medical information using the Meta Pixel tracking code on Defendant's Web Properties.

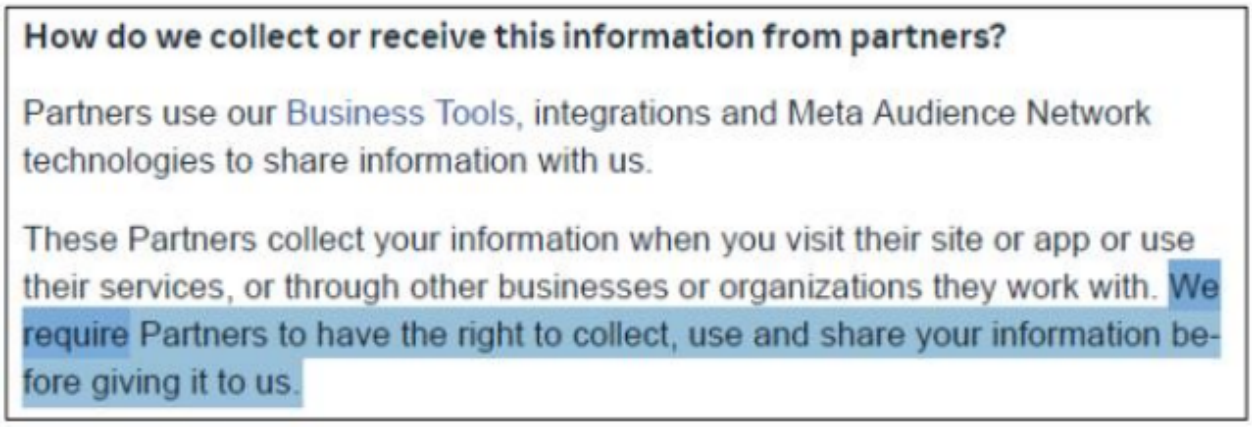
I. Defendant Knew Plaintiffs' Private Information Included Sensitive Medical Information, Including Medical Records.

217. By virtue of how the Meta Pixel works, i.e., sending all interactions on a website to Facebook, Defendant was aware that its Users' Private Information would be sent to Facebook when they researched specific medical conditions and/or treatments, looked up providers, made appointments, typed specific medical queries into the search bar, and otherwise interacted with Defendant's Web Properties.

> **Information from partners.**
> Advertisers, app developers, and publishers can send us information through Meta Business Tools they use, including our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel. These partners provide information about your activities off of our Products—including information about your device, websites you visit, purchases you make, the ads you see, and how you use their services —whether or not you have an account or are logged into our Products. For example, a game developer could use our API to tell us what games you play, or a business could tell us about a purchase you made in its store. We also receive information about your online and offline actions and purchases from third-party data providers who have the rights to provide us with your information.
>
> Partners receive your data when you visit or use their services or through third parties they work with. We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us. Learn more about the types of partners we receive data from.
>
> To learn more about how we use cookies in connection with Meta Business Tools, review the Facebook Cookies Policy and Instagram Cookies Policy.

218. At all times relevant herein Meta notified its partners, including Defendant, to have the rights to collect, use, and share user data before providing any data to Meta.[55] Although Meta's intent is questionable, Defendant had been on notice of this Pixel-tracking ever since they activated such Pixel technology on its Web Properties.

219. Meta changed this provision again in July 2022, while still requiring partners to have the right to share patient information with Meta:[56]



How do we collect or receive this information from partners?

Partners use our Business Tools, integrations and Meta Audience Network technologies to share information with us.

These Partners collect your information when you visit their site or app or use their services, or through other businesses or organizations they work with. We require Partners to have the right to collect, use and share your information before giving it to us.

220. Defendant had the explicit option to disable the Pixel technology on its Web Properties, but chose not to exercise this option, thereby continuing to share data with Facebook despite the availability of preventive measures.

221. Meta advised third party entities, like Defendant, to refrain from sending any information they did not have the legal right to send and expressly emphasized not to transmit health information. Yet, Defendant, in direct contravention of these disclosures, and more importantly despite Defendant's promises to keep all health-related data about patients

[55] *See In re Meta Pixel Healthcare Litig.*, No. 22-cv-03580-WHO, 2022 U.S. Dist. LEXIS 230754, at *13-14 (N.D. Cal. Dec. 22, 2022).

[56] Meta, *Data Policy: Information from Partners, vendors and third parties* (Jan. 1, 2023), https://www.facebook.com/privacy/policy?subpage=1.subpage.4-InformationFromPartnersVendors.

confidential, continued to employ Pixel tracking on its Web Properties, thereby sharing sensitive patient data without proper authorization or consent.

J. Plaintiffs and Class Members Have a Reasonable Expectation of Privacy in Their Private Information, Especially with Respect to Sensitive Medical Information.

222. Plaintiffs and Class Members have a reasonable expectation of privacy in their Private Information, including personal information and sensitive medical information.

223. HIPAA sets national standards for safeguarding protected health information. For example, HIPAA limits the permissible uses of health information and prohibits the disclosure of this information without explicit authorization. See 45 C.F.R. § 164.HIPAA also requires that covered entities implement appropriate safeguards to protect this information. See 45 C.F.R. § 164.530(c)(1).

224. This federal legal framework applies to health care providers, including Defendant.

225. Given the application of HIPAA to the Defendant, Plaintiffs and the members of the Class had a reasonable expectation of privacy over their PHI.

226. Several studies examining the collection and disclosure of consumers' sensitive medical information confirm that the collection and unauthorized disclosure of sensitive medical information from millions of individuals, as Defendant have done here, violates expectations of privacy that have been established as general societal norms.

227. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' data.

228. For example, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to obtain consent before selling or sharing consumers' data, and the same percentage believe internet companies and websites

should be required to provide consumers with a complete list of the data that has been collected about them.[57] Moreover, according to a study by Pew Research Center, a majority of Americans, approximately 79%, are concerned about how data is collected about them by companies.[58]

229. Users act consistent with these preferences. Following a new rollout of the iPhone operating software—which asks users for clear, affirmative consent before allowing companies to track users—85% of worldwide users and 94% of U.S. users chose not to share data when prompted.[59]

230. Medical data is particularly even more valuable because unlike other personal information, such as credit card numbers which can be quickly changed, medical data is static. This is why companies possessing medical information, like Defendant, are intended targets of cyber-criminals.[60]

231. Patients using Defendant's Web Properties must be able to trust that the information they input including their physicians, their health conditions and courses of treatment will be protected.

---

[57] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety/.

[58] *Americans and Privacy: Concerned, Confused, and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (November 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[59] Margaret Taylor, *How Apple Screwed Facebook*, WIRED (May 19, 2021), https://www.wired.co.uk/article/apple-ios14-facebook.

[60] Caroline Humer & Jim Finkle, *Your medical record is worth more to hackers than your credit card*, REUTERS (September 24, 2014), https://www.reuters.com/article/us-cybersecurity-hospitals/your-medical-record-is-worth-more-to-hackers-than-your-credit-card-idUSKCN0HJ21I20140924.

232. Indeed, numerous state and federal laws require this. And these laws are especially important when protecting individuals with particular medical conditions such as HIV or AIDS that can and do subject them to regular discrimination.

233. Furthermore, millions of Americans keep their health information private because it can become the cause of ridicule and discrimination. For instance, despite the anti-discrimination laws, persons living with HIV/AIDS are routinely subject to discrimination in healthcare, employment, and housing.[61]

234. The concern about sharing medical information is compounded by the reality that advertisers view this type of information as particularly high value. Indeed, having access to the data women share with their healthcare providers allows advertisers to obtain data on children before they are even born.

235. As one article put it: "the datafication of family life can begin from the moment in which a parent thinks about having a baby."[62] The article continues, "[c]hildren today are the very first generation of citizens to be datafied from before birth, and we cannot foresee —as yet— the social and political consequences of this historical transformation. What is particularly worrying about this process of datafication of children is that companies like . . . Facebook . . . are harnessing

[61] Bebe J. Anderson, JD, *HIV Stigma and Discrimination Persist, Even in Health Care*, AMA J. ETHICS (December 2009), https://journalofethics.ama-assn.org/article/hiv-stigma-and-discrimination-persist-even-health-care/2009-12.

[62] Veronica Barassi, *Tech Companies Are Profiling Us From Before Birth*, MIT PRESS READER (January 14, 2021), https://thereader.mitpress.mit.edu/tech-companies-are-profiling-us-from-before-birth/.

and collecting multiple typologies of children's data and have the potential to store a plurality of data traces under unique ID profiles."[63]

236. Other privacy law experts have expressed concerns about the disclosure to third parties of a users' sensitive medical information. For example, Dena Mendelsohn—the former Senior Policy Counsel at Consumer Reports and current Director of Health Policy and Data Governance at Elektra Labs—explained that having your personal health information disseminated in ways you are unaware of could have serious repercussions, including affecting your ability to obtain life insurance and how much you pay for that coverage, increase the rate you are charged on loans, and leave you vulnerable to workplace discrimination.[64]

237. Defendant surreptitiously collected and used Plaintiffs' and Class Members' Private Information, including highly sensitive medical information, through Meta Pixel in violation of Plaintiffs' and Class Members' privacy interests.

K. Atrium Was Enriched & Benefitted from the Use of the Pixel & other Tracking Technologies that Enabled the Unauthorized Disclosures Alleged Herein.

238. Meta advertises its' Pixel as a piece of code "that can help you better understand the effectiveness of your advertising and the actions people take on your site, like visiting a page or adding an item to their cart. You'll also be able to see when customers took an action after seeing your ad on Facebook and Instagram, which can help you with retargeting. And when you

---

[63] *Id.*

[64] *See* Class Action Complaint, *Jane Doe v. Regents of the Univ. of Cal. d/b/a UCSF Medical Center*, CLASS ACTION (Feb. 9, 2023), https://www.classaction.org/media/doe-v-regents-of-the-university-of-california.pdf.

use the Conversions API alongside the Pixel, it creates a more reliable connection that helps the delivery system decrease your costs."[65]

239. Retargeting is a form of online marketing that targets users with ads based on previous internet communications and interactions. Retargeting operates through code and tracking pixels placed on a website and cookies to track website visitors and then places ads on other websites the visitor goes to later.[66]

240. The process of increasing conversions and retargeting occurs in the healthcare context by sending a successful action on a health care website back to Facebook via the tracking technologies and the Pixel embedded on, in this case, Defendant's Website.

241. Through this process, the Meta Pixel loads and captures as much data as possible when a User loads a healthcare website that has installed the Pixel. The information the Pixel captures, "includes URL names of pages visited, and actions taken - all of which could be potential examples of health information."[67]

242. In exchange for disclosing the Private Information of their patients, Atrium is compensated by Facebook and likely other third parties in the form of enhanced advertising services and more cost-efficient marketing on their platform.

---

[65] *What is the Meta Pixel,* https://www.facebook.com/business/tools/meta-pixel (emphasis added) (last visited Apr. 4, 2024).

[66] *The complex world of healthcare retargeting,* https://www.medicodigital.com/the-complicated-world-of-healthcare-retargeting/ (last visited Apr. 4, 2024).

[67] *Id*.

243. But companies have started to warn about the potential HIPAA violations associated with using pixels and tracking technologies because many are not HIPAA-complaint or are only HIPAA-compliant if certain steps are taken.[68]

244. For example, Freshpaint a healthcare marketing vendor, cautioned that "Meta isn't HIPAA-compliant", and "If you followed the Facebook (or other general) documentation to set up your ads and conversion tracking using the Meta Pixel, remove the Pixel now."[69]

245. Medico Digital also warns that "retargeting requires sensitivity, logic and intricate handling. When done well, it can be a highly effective digital marketing tool. But when done badly, it could have serious consequences."[70]

246. Thus, utilizing the Pixels directly benefits Atrium by, among other things, reducing the cost of advertising and retargeting.

L. Plaintiffs' & Class Members' Private Information Has Substantial Value.

247. Plaintiffs' and Class Members' Private Information had value, and Defendant's disclosure and interception harmed Plaintiffs and the Class by not compensating them for the value of their Private Information and in turn decreasing the value of their Private Information.

248. The value of personal data is well understood and generally accepted as a form of currency. It is now incontrovertible that a robust market for this data undergirds the tech economy.

---

[68] *See* PIWIK Pro, *The guide to HIPAA compliance in analytics,* https://campaign.piwik.pro/wp-content/uploads/2023/10/The-guide-to-HIPAA-compliance-in-analytics.pdf (explaining that Google Analytics 4 is not HIPAA-compliant) (last visited Apr. 4, 2024).

[69] *Id*.

[70] *The complex world of healthcare retargeting, supra*, note 66.

249. The robust market for Internet user data has been analogized to the "oil" of the tech industry.[71] A 2015 article from TechCrunch accurately noted that "Data has become a strategic asset that allows companies to acquire or maintain a competitive edge."[72] That article noted that the value of a single Internet user—or really, a single user's data—varied from about $15 to more than $40.

250. Conservative estimates suggest that in 2018, Internet companies earned $202 per American user from mining and selling data. That figure is only due to keep increasing; estimates for 2022 are as high as $434 per user, for a total of more than $200 billion industry wide.

251. This economic value has been leveraged largely by corporations who pioneered the methods of its extraction, analysis and use.

252. However, the data also has economic value to Internet users. Market exchanges have sprung up where individual users like Plaintiffs herein can sell or monetize their own data. For example, Nielsen Data and Mobile Computer will pay Internet users for their data.[73]

253. Healthcare data is particularly valuable on the black market because it often contains all of an individual's PII and medical conditions as opposed to a single piece of information that may be found in a financial breach.

254. In 2023, the Value Examiner published a report that focused on the rise in providers, software firms and other companies that are increasingly seeking to acquire clinical

---

[71] *See The world's most valuable resource is no longer oil, but data*, https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (last visited Apr. 4, 2024).

[72] *See* https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/ (last visited Apr. 4, 2024).

[73] *See 10 Apps for Seling Your Data for* Cash, https://wallethacks.com/apps-for-selling-your-data/ (last visited Apr. 4, 2024).

patient data from healthcare organizations. The report cautioned providers that they must de-identify data and that purchasers and sellers of "such data should ensure it is priced at fair market value to mitigate any regulatory risk."[74]

255. In 2021, Trustwave Global Security published a report entitled Hackers, breaches and the value of healthcare data. With respect to healthcare data records, the report found that they may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card).[75]

256. The value of health data has also been reported extensively in the media. For example, Time Magazine published an article in 2017 titled "How Your Medical Data Fuels a Hidden Multi-Billion Dollar Industry," in which it described the extensive market for health data and observed that the market for information was both lucrative and a significant risk to privacy.[76]

257. Similarly, CNBC published an article in 2019 in which it observed that "[d]e-identified patient data has become its own small economy: There's a whole market of brokers who compile the data from providers and other health-care organizations and sell it to buyers."[77]

258. The dramatic difference in the price of healthcare data when compared to other forms of private information that is commonly sold is evidence of the value of PHI.

---

[74] *See Valuing Healthcare Data*, https://www.healthcapital.com/researchmaterialdocuments/publishedarticles/Valuing%20Healthcare%20Data.pdf (last visited Apr. 4, 2024).

[75] *See* https://www.imprivata.com/blog/healthcare-data-new-prize-hackers (citing *The Value of Data*, https://www.infopoint-security.de/media/TrustwaveValue_of_Data_Report_Final_PDF.pdf) (last visited Apr. 4, 2024).

[76] *See* https://time.com/4588104/medical-data-industry/ (last visited Apr. 4, 2024).

[77] *See* https://www.cnbc.com/2019/12/18/hospital-execs-say-theyre-flooded-with-requests-for-your-health-data.html (last visited Apr. 4, 2024).

259. But these rates are assumed to be discounted because they do not operate in competitive markets, but rather, in an illegal marketplace. If a criminal can sell other Internet users' stolen data, surely Internet users can sell their own data.

260. In short, there is a quantifiable economic value to Internet users' data that is greater than zero. The exact number will be a matter for experts to determine.

TOLLING, CONCEALMENT & ESTOPPEL

261. The applicable statutes of limitation have been tolled as a result of Defendant's knowing and active concealment and denial of the facts alleged herein.

262. Defendant secretly incorporated the Meta Pixel into its Web Properties and patient portals, providing no indication to Users that their User Data, including their Private Information, would be disclosed to unauthorized third parties.

263. Defendant had exclusive knowledge that the Meta Pixel was incorporated on its Web Properties, yet failed to disclose that fact to Users, or inform them that by interacting with its Web Properties, Plaintiffs' and Class Members' User Data, including Private Information, would be disclosed to third parties, including Facebook.

264. Plaintiffs and Class Members could not with due diligence have discovered the full scope of Defendant's conduct because the incorporation of Meta Pixels is highly technical and there were no disclosures or other indications that would inform a reasonable consumer that Defendant was disclosing and allowing Facebook to intercept Users' Private Information.

265. The earliest Plaintiffs and Class Members could have known about Defendant's conduct was approximately in June of 2022. Nevertheless, at all material times herein, Defendant falsely represented to Plaintiffs that their health information is not and will not be disclosed to any third party.

266. As alleged above, Defendant has a duty to disclose the nature and significance of its data disclosure practices but failed to do so. Defendant is therefore estopped from relying on any statute of limitations under the discovery rule.

CLASS ALLEGATIONS

267. **Class Definition:** Plaintiffs bring this action on behalf of themselves and on behalf of various classes of persons similarly situated, as defined below, pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.:

268. The Nationwide Class that Plaintiffs seek to represent is defined as:

> **Nationwide Class**: All individuals residing in the United States whose Private Information was disclosed to a third party without authorization or consent through the Meta Pixel on Defendant's Web Properties.

269. The Nationwide Class, is referred to throughout this Complaint as the "Class." Excluded from the Class are Defendant, its agents, affiliates, parents, subsidiaries, any entity in which Defendant has a controlling interest, any Defendant's officer or director, any successor or assign and any Judge who adjudicates this case, including their staff and immediate family.

270. **The following people are excluded from the Class:** (1) any Judge or Magistrate presiding over this action and members of their immediate families; (2) Defendant, Defendant's subsidiaries, parents, successors, predecessors, and any entity in which the Defendant or its parents have a controlling interest and its current or former officers and directors; (3) persons who properly execute and file a timely request for exclusion from the Class; (4) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (5) Plaintiffs' counsel and Defendant's counsel; and (6) the legal representatives, successors, and assigns of any such excluded persons.

271. Plaintiffs reserve the right under Federal Rule of Civil Procedure 23 to amend or modify the Class to include a broader scope, greater specificity, further division into subclasses, or limitations to particular issues. Plaintiffs reserve the right under Federal Rule of Civil Procedure 23(c)(4) to seek certification of particular issues.

272. The requirements of Federal Rules of Civil Procedure 23(a), 23(b)(2), and 23(b)(3) are met in this case.

273. **Numerosity**: The exact number of Class Members is not available to Plaintiffs, but it is clear that individual joinder is impracticable. Hundreds of thousands to millions of people have used Atrium's Web Properties since at least 2015. Members of the Class can be identified through Defendant's records or by other means.

274. **Commonality**: Commonality requires that the Class Members' claims depend upon a common contention such that determination of its truth or falsity will resolve an issue that is central to the validity of each claim in one stroke. Here, there is a common contention for all Class Members as to whether Defendant disclosed to third parties their Private Information without authorization or lawful authority.

275. **Typicality**: Plaintiffs' claims are typical of the claims of other Class Members in that Plaintiffs and the Class Members sustained damages arising out of Defendant's uniform wrongful conduct and data sharing practices.

276. **Adequate Representation**: Plaintiffs will fairly and adequately represent and protect the interests of the Class Members. Plaintiffs' claims are made in a representative capacity on behalf of the Class Members. Plaintiffs have no interests antagonistic to the interests of the other Class Members. Plaintiffs have retained competent counsel to prosecute the case on behalf

of Plaintiffs and the Class. Plaintiffs and Plaintiffs' counsel are committed to vigorously prosecuting this action on behalf of the Class members.

277. The declaratory and injunctive relief sought in this case includes:

a. Entering a declaratory judgment against Defendant—declaring that Defendant's interception of Plaintiffs' and Class Members' Private Information is in violation of the law;

b. Entering an injunction against Defendant:

i. preventing Defendant from sharing Plaintiffs' and Class Members' Private Information among itself and other third parties;

ii. requiring Defendant to alert and/or otherwise notify all Users of its Web Properties of what information is being collected, used, and shared;

iii. requiring Defendant to provide clear information regarding its practices concerning data collection from the Users/patients of Defendant's Web Properties, as well as uses of such data;

iv. requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information

v. and requiring Defendant to provide an opt out procedure for individuals who do not wish for their information to be tracked while interacting with Defendant's Web Properties.

278. **Predominance**: There are many questions of law and fact common to the claims of Plaintiffs and Class Members, and those questions predominate over any questions that may affect individual Class Members. Common questions and/or issues for Class members include, but are not necessarily limited to the following:

a. Whether Defendant's unauthorized disclosure of Users' Private Information was negligent;

b. Whether Defendant owed a duty to Plaintiffs' and Class Members not to disclose their Private Information to unauthorized third parties;

c. Whether Defendant breached its duty to Plaintiffs and Class Members not to disclose their Private Information to unauthorized third parties;

d. Whether Defendant represented to Plaintiffs and the Class that it would protect Plaintiff's and the Class Members' Private Information;

e. Whether Defendant violated Plaintiffs' and Class Members' privacy rights;

f. Whether Plaintiffs and Class Members are entitled to actual damages, enhanced damages, statutory damages, and other monetary remedies provided by equity and law and

g. Whether injunctive and declaratory relief, restitution, disgorgement, and other equitable relief is warranted.

279. **Superiority:** This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by individual Class Members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would be virtually impossible for the individual Class Members to obtain effective relief from Defendant's misconduct. Even if Class Members could mount such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single Court. Economies of time, effort and expense will be enhanced, and uniformity of decisions ensured.

280. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant misrepresented that it would disclose personal information only for limited purposes that did not include purposes of delivering advertisements

or collecting data for commercial use or supplementing consumer profiles created by data aggregators and advertisers;

b. Whether Defendant's privacy policies misrepresented that it collected and shared User information with third-party service providers only for the limited purpose of providing access to its services;

c. Whether Defendant misrepresented that it had in place contractual and technical protections that limit third-party use of User information and that it would seek User consent prior to sharing Private Information with third parties for purposes other than provision of its services;

d. Whether Defendant misrepresented that any information it receives is stored under the same guidelines as any health entity that is subject to the strict patient data sharing and protection practices set forth in the regulations propounded under HIPAA;

e. Whether Defendant misrepresented that it complied with HIPAA's requirements for protecting and handling Users' PHI;

f. Whether Defendant breached its contractual obligations to not share Users' PHI without express written authorization;

g. Whether Defendant shared the Private Information that Users provided to Defendant with advertising platforms, including Facebook, without adequate notification or disclosure, and without Users' consent, in violation of health privacy laws and rules and its own privacy policy;

h. Whether Defendant integrated third-party tracking tools, such as Pixels, in its website that shared Private Information and User activities with third parties for unrestricted purposes, which included advertising, data analytics, and other commercial purposes;

i. Whether Defendant shared Private Information and activity information with Facebook using Facebook's Pixels on its Web Properties without Users' consent and

j. Whether Facebook used the information that Defendant shared with it for unrestricted purposes, such as selling targeted advertisements, data analytics, and other commercial purposes.

CAUSES OF ACTION

COUNT ONE

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT
18 U.S.C. § 2511(1), *et seq*.
Unauthorized Interception, Use and Disclosure
(*On Behalf of Plaintiffs & the Nationwide Class*)

281. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

282. The ECPA prohibits the intentional interception of the content of any electronic communication. 18 U.S.C. § 2511.

283. The ECPA protects both sending and receipt of communications.

284. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire or electronic communications are intercepted, disclosed, or intentionally used in violation of Chapter 119.

285. The transmissions of Plaintiffs' PII and PHI to Defendant's Web Properties qualify as "communications" under the ECPA's definition of 18 U.S.C. § 2510(12).

286. **Electronic Communications**. The transmission of PII and PHI between Plaintiffs and Class Members and Defendant's Web Properties with which they chose to exchange communications are "transfer[s] of signs, signals, writing,…data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate commerce" and are therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(2).

287. **Content**. The ECPA defines content, when used with respect to electronic communications, to "include[] any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8) (emphasis added).

288. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding PII and PHI, diagnosis of certain conditions, treatment/medication for such conditions, and scheduling of appointments, including annual mammograms, surgeries, ER visits, lab work, and scans.

289. Furthermore, Defendant intercepted the "contents" of Plaintiffs' communications in at least the following forms:

a. The parties to the communications;

b. The precise text of patient search queries;

c. PII such as patients' IP addresses, Facebook IDs, browser fingerprints, and other unique identifiers;

d. The precise text of patient communications about specific doctors;

e. The precise text of patient communications about specific medical conditions;

f. The precise text of information generated when patients requested or made appointments,

g. The precise text of patient communications about specific treatments;

h. The precise text of patient communications about scheduling appointments with medical providers;

i. The precise text of patient communications about billing and payment;

j. The precise text of specific buttons on Defendant's Web Properties that patients click to exchange communications including Log-Ins, Registrations, Requests for Appointments, Search, and other buttons;

k. The precise dates and times when patients click to Log-In on Defendant's Web Properties;

l. The precise dates and times when patients visit Defendant's Web Properties;

m. Information that is a general summary or informs third parties of the general subject of communications that Defendant sends back to patients in response to search queries and requests for information about specific doctors, conditions, treatments, billing, payment, and other information.

290. For example, Defendant's interception of the fact that a patient views a webpage like:

https://atriumhealth.org/medical-services/specialty-care/heart-care?isMobileWidget=false&cityName=&community=All_Communities&locationName=&pageNumber=&pageSize=10&latitude=35.2270869&longitude=-80.8431267&sortBy=&datasource=5c4b1d04-706d-45ae-81e1-66f1add7b7f5&childrensLocationOnly=false&locationType=Heart_Care

involves "content," because it communicates that patient's request for the information on that page.

291. **Interception**. The ECPA defines the interception as the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device" and "contents … include any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(4), (8).

292. **Electronical, Mechanical or Other Device**. The ECPA defines "electronic, mechanical, or other device" as "any device … which can be used to intercept a[n] … electronic communication[.]" 18 U.S.C. § 2510(5). The following constitute "devices" within the meaning of 18 U.S.C. § 2510(5):

a. The cookies Atrium and Meta use to track Plaintiffs' and the Class Members' communications;

b. Plaintiffs' and Class Members' browsers;

c. Plaintiffs' and Class Members' computing devices

d. Defendant's web servers and

e. The Pixel code deployed by Defendant to effectuate the sending and acquisition of patient communications.

293. By utilizing and embedding the Pixel on its Web Properties, Defendant intentionally intercepted, endeavored to intercept, and procured another person to intercept, the

electronic communications of Plaintiffs and Class Members, in violation of 18 U.S.C. § 2511(1)(a).

294. Specifically, Defendant intercepted Plaintiffs' and Class Members' electronic communications via the Pixel, which tracked, stored, and unlawfully disclosed Plaintiffs' and Class Members' Private Information to third parties such as Facebook.

295. Defendant's intercepted communications include, but are not limited to, communications to/from Plaintiffs and Class Members regarding PII and PHI, treatment, medication, and scheduling.

296. This information was, in turn, used by third parties, such as Facebook to 1) place Plaintiffs and Class Members in specific health-related categories and 2) target Plaintiffs and Class Members with advertising associated with their specific health conditions.

297. By intentionally disclosing or endeavoring to disclose the electronic communications of Plaintiffs and Class Members to affiliates and other third parties, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(c).

298. By intentionally using, or endeavoring to use, the contents of the electronic communications of Plaintiffs and Class Members, while knowing or having reason to know that the information was obtained through the interception of an electronic communication in violation of 18 U.S.C. § 2511(1)(a), Defendant violated 18 U.S.C. § 2511(1)(d).

299. Unauthorized Purpose. Defendant intentionally intercepted the contents of Plaintiffs' and Class Members' electronic communications for the purpose of committing a

tortious act in violation of the Constitution or laws of the United States or of any State—namely, violation of HIPAA and the causes of action described below, among others.

300. The ECPA provides that a "party to the communication" may liable where a "communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." 18 U.S.C § 2511(2)(d).

301. Defendant is not a party for purposes to the communication based on its unauthorized duplication and transmission of communications with Plaintiffs and the Class. However, even assuming Defendant is a party, Defendant's simultaneous, unknown duplication, forwarding, and interception of Plaintiffs' and Class Members' Private Information does not qualify for the party exemption.

302. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing IIHI to a third party.

303. HIPAA defines IIHI as:

> any information, including demographic information collected from an individual, that—(A) is created or received by a health care provider ... (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and (i) identifies the individual; or (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

304. Plaintiffs' and Class Members' information that Defendant disclosed to third parties qualifies as IIHI, and Defendant violated Plaintiff's expectations of privacy, and constitutes tortious and/or criminal conduct through a violation of 42 U.S.C. § 1320d(6). Defendant intentionally used the wire or electronic communications to intercept Plaintiffs Private Information in violation of the law.

305. Defendant's conduct violated 42 U.S.C. § 1320d-6 in that it: Used and caused to be used cookie identifiers associated with specific patients without patient authorization; and disclosed individually identifiable health information to Facebook without patient authorization.

306. The penalty for violation is enhanced where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." 42 U.S.C. § 1320d-6.

307. Defendant's conduct would be subject to the enhanced provisions of 42 U.S.C. § 1320d-6 because Defendant's use of the Facebook source code was for Defendant's commercial advantage to increase revenue from existing patients and gain new patients.

308. Defendant's acquisition of patient communications that were used and disclosed to Facebook was also done for purposes of committing criminal and tortious acts in violation of the laws of the United States and individual States nationwide as set forth herein, including:

a. Negligence;

b. Breach of express contract;

c. Breach of implied contract; and

d. Breach of fiduciary duty.

309. Defendant is not exempt from ECPA liability under 18 U.S.C. § 2511(2)(d) on the ground that it was a participant in Plaintiffs' and Class Members' communications about their Private Information on its Web Properties, because it used its participation in these communications to improperly share Plaintiffs' and Class Members' Private Information with Facebook and third-parties that did not participate in these communications, that Plaintiffs and Class Members did not know was receiving their information, and that Plaintiffs and Class Members did not consent to receive this information.

310. Here, as alleged above, Defendant violated a provision of HIPAA, specifically 42 U.S.C. § 1320d-6(a)(3). This provision imposes a criminal penalty for knowingly disclosing individually identifiable health information to a third party.

311. As such, Defendant cannot viably claim any exception to ECPA liability.

312. Plaintiffs and Class Members have suffered damages as a direct and proximate result of Defendant's invasion of privacy in that:

a. Learning that Defendant has intruded upon, intercepted, transmitted, shared, and used their PII and PHI (including information about their medical symptoms, conditions, and concerns, medical appointments, healthcare providers and locations, medications and treatments, and health insurance and medical bills) for commercial purposes has caused Plaintiffs and the Class Members to suffer emotional distress;

b. Defendant received substantial financial benefits from its use of Plaintiffs' and the Class Members' PII and PHI without providing any value or benefit to Plaintiffs or the Class members;

c. Defendant received substantial, quantifiable value from its use of Plaintiffs' and the Class Members' PII and PHI, such as understanding how people use its Web Properties and determining what ads people see on its Web Properties, without providing any value or benefit to Plaintiffs or the Class Members;

d. Defendant has failed to provide Plaintiffs and the Class Members with the full value of the medical services for which they paid, which included a duty to maintain the confidentiality of its patient information and

e. The diminution in value of Plaintiffs' and Class Members' PII and PHI and the loss of privacy due to Defendant making sensitive and confidential information, such as patient status, medical treatment, and appointments that Plaintiffs and Class Members intended to remain private no longer private.

313. Defendant intentionally used the wire or electronic communications to increase its profit margins. Defendant specifically used the Pixel to track and utilize Plaintiffs' and Class Members' Private Information for financial gain.

314. Defendant was not acting under color of law to intercept Plaintiffs' and the Class Members' wire or electronic communication.

315. Plaintiffs and Class Members did not authorize Defendant to acquire the content of their communications for purposes of invading their privacy via the Pixel.

316. Any purported consent that Defendant received from Plaintiffs and Class Members was not valid.

317. Consumers have the right to rely upon the promises that companies make to them. Defendant accomplished its tracking and retargeting through deceit and disregard, such that an actionable claim may be made, in that it was accomplished through source code that caused third-party Pixels and cookies (including but not limited to the fbp, ga and gid cookies) and other tracking technologies to be deposited on Plaintiffs' and Class members' computing devices as "first-party" cookies that are not blocked.

318. Defendant's scheme or artifice to defraud in this action consists of:

a. the false and misleading statements and omissions in its privacy policy set forth above, including the statements and omissions recited in the claims below; and

b. the placement of the 'fbp' cookie on patient computing devices disguised as a first-party cookie on Defendant's Website rather than a third-party cookie from Facebook.

319. Defendant acted with the intent to defraud in that it willfully invaded and took Plaintiffs' and Class Members' property:

a. property rights to the confidentiality of Private Information and their right to determine whether such information remains confidential and exclusive right to determine who may collect and/or use such information for marketing purposes; and

b. property rights to determine who has access to their computing devices.

320. In sending and in acquiring the content of Plaintiffs' and Class Members' communications relating to the browsing of Defendant's Web Properties, Defendant's purpose was tortious, criminal, and designed to violate federal and state legal provisions including a

knowing intrusion into a private, place, conversation, or matter that would be highly offensive to a reasonable person.

321. As a result of Defendant's violation of the ECPA, Plaintiffs and the Class are entitled to all damages available under 18 U.S.C. § 2520, including statutory damages of whichever is the greater of $100 a day for each day of violation or $10,000, equitable or declaratory relief, compensatory and punitive damages, and attorney's fees and costs.

COUNT TWO

BREACH OF EXPRESS CONTRACT
(On behalf of Plaintiffs & the Nationwide Class)

322. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

323. Plaintiffs and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of medical and health care services.

324. Specifically, Plaintiffs and Class Members entered into a valid and enforceable express contract with Defendant when Plaintiffs first received medical care from Defendant.

325. The valid and enforceable express contracts to provide medical and health care services that Plaintiffs and Class Members entered into with Defendant include Defendant's promise to protect nonpublic, Private Information given to Defendant or that Defendant gathers on their own from disclosure.

326. Under these express contracts, Defendant and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members; and (b) protect Plaintiffs and the Class Members' PII/PHI: (i) provided to obtain such healthcare;

and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

327. Both the provision of medical services and the protection of Plaintiffs and Class Members' Private Information were material aspects of these express contracts.

328. The express contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiffs and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

329. At all relevant times, Defendant expressly represented in its Privacy Notice, among other things: (i) that "[a]t Atrium Health, we understand that your health information is personal and we are committed to protecting your privacy"; and (ii) that "[b]efore we use or share your health information for a purpose that is not covered by this Notice or required or permitted by law, we will ask for your written permission. For example, we will ask for your authorization . . . to use your health information for marketing purposes, or to share your information in a way that would be considered the sale of health information."[78]

330. Defendant's express representations, including, but not limited to, express representations found in their Privacy Notice, formed and embodied an express contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

331. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry

[78] https://atriumhealth.org/for-patients-visitors/privacy/english (last visited Apr. 4, 2024).

standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

332. Plaintiffs and Class Members would not have entered into these contracts with Defendant and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

333. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

334. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

335. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel on its Web Properties.

336. Defendant materially breached the terms of these express contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with Meta through the Meta Collection Tools, including the Meta Pixel on its Web Properties.

337. The mass and systematic disclosure of Plaintiffs' and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

338. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts.

339. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

340. Had Defendant disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or their affiliated healthcare providers.

341. As a direct and proximate result of the disclosure of Plaintiffs' and Class Members' Private Information to Meta, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

342. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiffs' and Class Members' Private Information to Meta.

COUNT THREE

BREACH OF IMPLIED DUTY OF GOOD FAITH AND FAIR DEALING
(On behalf of Plaintiffs & the Nationwide Class)

343. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

344. Plaintiffs and Class Members allege they entered into valid and enforceable express contracts or were third-party beneficiaries of valid and enforceable express contracts, with Defendant for the provision of medical and health care services.

345. Specifically, Plaintiffs and Class Members entered into a valid and enforceable express contract with Defendant when Plaintiffs first received medical care from Defendant.

346. The valid and enforceable express contracts to provide medical and health care services that Plaintiffs and Class Members entered into with Defendant include Defendant's implied duty of good faith and fair dealing, particularly due to Defendant's special relationship with Plaintiffs as their healthcare provider.

347. Under these express contracts, Defendant and/or their affiliated healthcare providers, promised and were obligated to provide healthcare to Plaintiffs and Class Members. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

348. In service of its implied duty of good faith and fair dealing when executing the contract, Defendant was bound to not voluntarily divulge Plaintiffs' and Class Members' sensitive, non-public Private Information to third parties for monetary gain without Plaintiff's and Class Members' consent to such disclosures.

349. The express contracts for the provision of medical services are formed and embodied in multiple documents.

350. As evidence of Defendant's knowledge of its obligations to perform the contracts in accordance with its implied duty of good faith and fair dealing and Plaintiffs' expectations of Defendant to do the same, at all relevant times, Defendant expressly represented in its Privacy Notice, among other things: (i) that "[a]t Atrium Health, we understand that your health information is personal and we are committed to protecting your privacy"; and (ii) that "[b]efore we use or share your health information for a purpose that is not covered by this Notice or required or permitted by law, we will ask for your written permission. For example, we will ask for your authorization . . . to use your health information for marketing purposes, or to share your information in a way that would be considered the sale of health information."[79]

351. Defendant's express representations, including, but not limited to, express representations found in their Privacy Notice, evidence Defendant's knowledge of the specific manifestations of its duty to perform the contracts in accordance with its implied duty of good faith and fair dealing, which required Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

352. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security.

353. Plaintiffs and Class Members would not have entered into these contracts with Defendant and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

[79] https://atriumhealth.org/for-patients-visitors/privacy/english (last visited Apr. 4, 2024).

354. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and, through Defendant's implied duty of good faith and fair dealing, the protection of their Private Information.

355. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

356. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with Meta through the Meta Collection Tools, including the Meta Pixel on its Web Properties.

357. Defendant breached its implied duty of good faith and fair dealing to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel on its Web Properties.

358. The mass and systematic disclosure of Plaintiffs' and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of its implied duty of good faith and fair dealing.

359. As a result of Defendant's failure to fulfill the data privacy protections inherent in the special relationship with Plaintiffs and the Class Members, and resulting breach of its implied duty of good faith and fair dealing, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts.

360. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

361. Had Defendant disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or their affiliated healthcare providers.

362. As a direct and proximate result of the disclosure of Plaintiffs' and Class Members' Private Information to Meta, Plaintiffs and Class Members have been harmed and have suffered, and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

363. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiffs' and Class Members' Private Information to Meta.

COUNT FOUR

BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs & the Nationwide Class)

364. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

365. Plaintiffs and Class Members allege they entered into valid and enforceable implied contracts or were third-party beneficiaries of valid and enforceable implied contracts, with Defendant for the provision of medical and health care services.

366. Specifically, Plaintiffs and Class Members entered into a valid and enforceable contract with Defendant when Plaintiffs first received medical care from Defendant.

367. The valid and enforceable contracts to provide medical and health care services that Plaintiffs and Class Members entered into with Defendant include Defendant's promise to protect nonpublic, Private Information given to Defendant or that Defendant gathers on their own from disclosure.

368. Under these contracts, Defendant and/or their affiliated healthcare providers, promised and were obligated to: (a) provide healthcare to Plaintiffs and Class Members; and (b) protect Plaintiffs and the Class Members' PII/PHI: (i) provided to obtain such healthcare; and/or (ii) created as a result of providing such healthcare. In exchange, Plaintiffs and Members of the Class agreed to pay money for these services, and to turn over their Private Information.

369. Both the provision of medical services and the protection of Plaintiffs and Class Members' Private Information were material aspects of these contracts.

370. The contracts for the provision of medical services – contracts that include the contractual obligations to maintain the privacy of Plaintiffs and Class Members' Private Information—are formed and embodied in multiple documents, including (among other documents) Defendant's Privacy Notice.

371. At all relevant times, Defendant expressly represented in its Privacy Notice, among other things: (i) that "[a]t Atrium Health, we understand that your health information is personal and we are committed to protecting your privacy"; and (ii) that "[b]efore we use or share your

health information for a purpose that is not covered by this Notice or required or permitted by law, we will ask for your written permission. For example, we will ask for your authorization . . . to use your health information for marketing purposes, or to share your information in a way that would be considered the sale of health information."[80]

372. Defendant's express representations, including, but not limited to, express representations found in their Privacy Notice, formed and embodied an express contractual obligation requiring Defendant to implement data security adequate to safeguard and protect the privacy of Plaintiffs' and Class Members' Private Information.

373. Consumers of healthcare value their privacy, the privacy of their dependents, and the ability to keep their Private Information associated with obtaining healthcare private. To customers such as Plaintiffs and Class Members, healthcare that does not adhere to industry standard data security protocols to protect Private Information is fundamentally less useful and less valuable than healthcare that adheres to industry-standard data security. Plaintiffs and Class Members would not have entered into these contracts with Defendant and/or their affiliated healthcare providers as a direct or third-party beneficiary without an understanding that their Private Information would be safeguarded and protected.

374. A meeting of the minds occurred, as Plaintiffs and Members of the Class agreed to and did provide their Private Information to Defendant and/or their affiliated healthcare providers, and paid for the provided healthcare in exchange for, amongst other things, both the provision of healthcare and medical services and the protection of their Private Information.

375. Plaintiffs and Class Members performed their obligations under the contract when they paid for their health care services and provided their Private Information.

[80] https://atriumhealth.org/for-patients-visitors/privacy/english (last visited Mar. 31, 2024).

376. Defendant materially breached its contractual obligation to protect the nonpublic Private Information Defendant gathered when it disclosed that Private Information to Meta through the Meta Collection Tools, including the Meta Pixel on its Web Properties.

377. Defendant materially breached the terms of these contracts, including, but not limited to, the terms stated in the relevant Privacy Notice. Defendant did not maintain the privacy of Plaintiffs' and Class Members' Private Information as evidenced by Defendant's sharing of that Private Information with Meta through the Meta Collection Tools, including the Meta Pixel on its Web Properties.

378. The mass and systematic disclosure of Plaintiffs' and Class Members' Private Information to third parties, including Meta, was a reasonably foreseeable consequence of Defendant's actions in breach of these contracts.

379. As a result of Defendant's failure to fulfill the data privacy protections promised in these contracts, Plaintiffs and Members of the Class did not receive the full benefit of the bargain, and instead received healthcare and other services that were of a diminished value to that described in the contracts. Plaintiffs and Class Members therefore were damaged in an amount at least equal to the difference in the value of the healthcare with data privacy protection they paid for and the healthcare they received.

380. Had Defendant disclosed that their data privacy was inadequate or that they did not adhere to industry-standard privacy measures, neither the Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or their affiliated healthcare providers.

381. As a direct and proximate result of the disclosure of Plaintiffs' and Class Members' Private Information to Meta, Plaintiffs and Class Members have been harmed and have suffered,

and will continue to suffer, actual damages and injuries, including without limitation the release, disclosure, and publication of their Private Information, the loss of control and diminution in value of their Private Information, the imminent risk of suffering additional damages in the future, disruption of their medical care and treatment, out-of-pocket expenses, and the loss of the benefit of the bargain they had struck with Defendant.

382. Plaintiffs and Class Members are entitled to compensatory and consequential damages suffered as a result of the disclosure of Plaintiffs' and Class Members' Private Information to Meta.

COUNT FIVE
NEGLIGENCE
(On behalf of Plaintiffs & the Nationwide Class)

383. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

384. Defendant required Plaintiffs and Class Members to submit non-public personal information in order to obtain healthcare services.

385. Upon accepting, storing, and controlling the Private Information of Plaintiffs and the Class in its computer systems, Defendant owed, and continues to owe, a duty to Plaintiffs and the Class to exercise reasonable care to secure, safeguard and protect their highly sensitive Private Information from disclosure to third parties.

386. Defendant's duty of care to use reasonable measures to secure and safeguard Plaintiffs' and Class Members' Private Information arose due, in part, to the special relationship that existed between Defendant and its patients, which is recognized by statute, regulations, and the common law.

387. In addition, Defendant had a duty under HIPAA privacy laws, which were enacted with the objective of protecting the confidentiality of clients' healthcare information and set forth the conditions under which such information can be used, and to whom it can be disclosed. HIPAA privacy laws not only apply to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient that—if it were to fall into the wrong hands—could present a risk of harm to the patient's finances or reputation.

388. Defendant's duty to use reasonable security measures under HIPAA required Defendant to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1).

389. Some or all of the healthcare, medical, and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

390. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

391. Defendant's duty to use reasonable care in protecting confidential data arose also because Defendant is bound by industry standards to protect confidential Private Information.

392. Defendant breached this duty by failing to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class Members' Private Information from unauthorized disclosure.

393. It was reasonably foreseeable that Defendant's failures to exercise reasonable care in safeguarding and protecting Plaintiffs' and Class members' Private Information through its use

of the Meta Pixels and other tracking technologies would result in unauthorized third parties, such as Facebook, gaining access to such Private Information for no lawful purpose.

394. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class Members and their Private Information.

395. Defendant's misconduct included the failure to (1) secure Plaintiffs' and Class Members' Private Information; (2) comply with industry standard data security practices; (3) implement adequate website and event monitoring; (4) implement the systems, policies, and procedures necessary to prevent unauthorized disclosures resulting from the use of the Meta Pixels and other tracking technologies; and (5) prevent unauthorized access to Plaintiffs' and Class Members' Private Information by sharing that information with Meta and other third parties. Defendant's failures and breaches of these duties constituted negligence.

396. As a direct result of Defendant's breach of its duty of confidentiality and privacy and the disclosure of Plaintiffs' and Class members' Private Information, Plaintiffs and the Class have suffered damages that include, without limitation, loss of the benefit of the bargain, increased infiltrations into their privacy through spam and targeted advertising they did not ask for, loss of privacy, loss of confidentiality, embarrassment, emotional distress, humiliation and loss of enjoyment of life.

397. Defendant's wrongful actions and/or inactions and the resulting unauthorized disclosure of Plaintiffs' and Class members' Private Information constituted (and continue to constitute) negligence at common law.

398. Plaintiffs and Class Members are entitled to compensatory, nominal, and/or punitive damages, and Plaintiffs and Class Members are entitled to recover those damages in an amount to be determined at trial.

399. Defendant's negligent conduct is ongoing, in that it still holds the Private Information of Plaintiffs and Class Members in an unsafe and unsecure manner. Therefore, Plaintiffs and Class Members are also entitled to injunctive relief requiring Defendant to (i) strengthen its data security systems and monitoring procedures; (ii) cease sharing Plaintiffs' and Class Members' Private Information with Meta and other third parties without Plaintiffs' and Class Members' express consent; and (iii) submit to future annual audits of its security systems and monitoring procedures.

COUNT SIX
BREACH OF FIDUCIARY DUTY
(*On Behalf of Plaintiffs & the Nationwide Class*)

400. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

401. In light of the special physician-patient relationship between Defendant and Plaintiffs and Class Members, which was created for the purpose of Defendant providing healthcare to Plaintiffs and Class Members, Defendant became guardian of Plaintiffs' and Class Members' Private Information. Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for Plaintiffs and Class Members, (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of an unauthorized disclosure; and (3) to maintain complete and accurate records of what information (and where) Defendant did and does store.

402. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of Defendant' relationship with its patients and former patients, in particular, to keep secure their Private Information.

403. Defendant breached its fiduciary duties to Plaintiffs and Class Members by disclosing their Private Information to unauthorized third parties, including Meta, and separately, by failing to notify Plaintiffs and Class Members of this fact.

404. As a direct and proximate result of Defendant' breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer injury and are entitled to compensatory, nominal, and/or punitive damages, and disgorgement of profits, in an amount to be proven at trial.

COUNT SEVEN
UNJUST ENRICHMENT
(On behalf of Plaintiffs & Nationwide Class)

405. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein, except for the paragraphs specifically regarding breach of contract.

406. Plaintiffs plead this claim in the alternative to their breach of contract claim.

407. Plaintiffs and Class Members personally and directly conferred a benefit on Defendant by paying Defendant for health care services, which included Defendant's obligation to protect Plaintiffs' and Class Members' Private Information. Defendant was aware of Plaintiffs' privacy expectations, and in fact, promised to maintain Plaintiffs' Private Information confidential and not to disclose to third parties. Defendant received payments for medical services from Plaintiffs and Class Members.

408. Plaintiffs and Class Members also conferred a benefit on Defendant in the form of valuable sensitive medical information that Defendant collected from Plaintiffs and Class Members under the guise of keeping this information private.

409. Defendant collected, used, and disclosed this information for its own gain, including for advertisement, market research, sale, or trade for valuable benefits from Facebook and other third parties.

410. Defendant had knowledge that Plaintiffs and Class Members had conferred this benefit on Defendant by interacting with its Web Properties, and Defendant intentionally installed the Meta Pixel tool on its Web Properties to capture and monetize this benefit conferred by Plaintiffs and Class Members.

411. Plaintiffs and Class Members would not have used Defendant's Web Properties had they known that Defendant would collect, use, and disclose this information to Facebook, Google, and other third parties.

412. The services that Plaintiffs and Class Members ultimately received in exchange for the monies paid to Defendant were worth quantifiably less than the services that Defendant promised to provide, which included Defendant's promise that any patient communications with Defendant would be treated as confidential and would never be disclosed to third parties for marketing purposes without the express consent of patients.

413. The medical services that Defendant offers are available from many other health care systems that do protect the confidentiality of patient communications. Had Defendant disclosed that it would allow third parties to secretly collect Plaintiffs' and Class Members' Private Health Information without consent, neither Plaintiffs, the Class Members, nor any reasonable person would have purchased healthcare from Defendant and/or its affiliated healthcare providers.

414. By virtue of the unlawful, unfair and deceptive conduct alleged herein, Defendant knowingly realized hundreds of millions of dollars in revenue from the use of the Private

Information of Plaintiffs and Classes Members for profit by way of targeted advertising related to Users' respective medical conditions and treatments sought.

415. This Private Information, the value of the Private Information, and/or the attendant revenue, were monetary benefits conferred upon Defendant by Plaintiffs and Class Members.

416. As a result of Defendant's conduct, Plaintiffs and Class Members suffered actual damages in the loss of value of their Private Information and the lost profits from the use of their Private Information.

417. It would be inequitable and unjust to permit Defendant to retain the enormous economic benefits (financial and otherwise) it has obtained from and/or at the expense of Plaintiffs and Class Members.

418. Defendant will be unjustly enriched if it is permitted to retain the economic benefits conferred upon them by Plaintiffs and Class Members through Defendant's obtaining the Private Information and the value thereof, and profiting from the unlawful, unauthorized and impermissible use of the Private Information of Plaintiffs and Class Members.

419. Plaintiffs and Class Members are therefore entitled to recover the amounts realized by Defendant at the expense of Plaintiffs and Class Members.

420. Plaintiffs and the Class Members have no adequate remedy at law and are therefore entitled to restitution, disgorgement, and/or the imposition of a constructive trust to recover the amount of Defendant's ill-gotten gains, and/or other sums as may be just and equitable.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and the Proposed Class defined herein, respectfully request this Honorable Court to provide the following relief:

A. That this Action be maintained as a Class Action, that Plaintiffs be named as Class Representative of the Class, that the undersigned be named as Lead Class Counsel of the Class, and that notice of this Action be given to Class Members;

B. That the Court enter an order:

1. Preventing Defendant from sharing Plaintiffs' and Class Members' Private Information among other third parties;

2. Requiring Defendant to alert and/or otherwise notify all Users of its Web Properties of what information is being collected, used, and shared;

3. Requiring Defendant to provide clear information regarding its practices concerning data collection from the Users/patients of Defendant's Web Properties, as well as uses of such data;

4. Requiring Defendant to establish protocols intended to remove all personal information which has been leaked to Facebook and/or other third parties, and request Facebook/third parties to remove such information;

5. Requiring Defendant to provide an opt out procedures for individuals who do not wish for their information to be tracked while interacting with Defendant's Web Properties;

6. Mandating the proper notice be sent to all affected individuals, and posted publicly;

7. Requiring Defendant to delete, destroy, and purge the Private Information of Users unless Defendant can provide reasonable justification for the retention and use of such information when weighed against the privacy interests of Users;

8. Requiring all further and just corrective action, consistent with permissible law and pursuant to only those causes of action so permitted.

C. That the Court award Plaintiffs and the Class Members damages (both actual damages for economic and non-economic harm and statutory damages) in an amount to be determined at trial;

D. That the Court issue appropriate equitable and any other relief (including monetary damages, restitution, and/or disgorgement) against Defendant to which Plaintiffs and the Class are entitled, including but not limited to restitution and an Order requiring Defendant to cooperate and financially support civil and/or criminal asset recovery efforts;

E. Plaintiffs and the Class be awarded with pre- and post-judgment interest (including pursuant to statutory rates of interest set under State law);

F. Plaintiffs and the Class be awarded with the reasonable attorneys' fees and costs of suit incurred by their attorneys;

G. Plaintiffs and the Class be awarded with treble and/or punitive damages insofar as they are allowed by applicable laws; and

H. Any and all other such relief as the Court may deem just and proper under the circumstances.

JURY TRIAL DEMANDED

Plaintiffs demand a jury trial on all triable issues.

DATED: April 10, 2024

Respectfully submitted,

s/ David M. Wilkerson
David M. Wilkerson
N.C. Bar Number 35742
THE VAN WINKLE LAW FIRM
11 N. Market Street
Asheville, NC 28801
(828) 258-2991
dwilkerson@vwlawfirm.com

s/ David S. Almeida
David S. Almeida
(*pro hac vice* admission to be sought)
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, Illinois 60614
(312) 576-3024 (phone)
david@almeidalawgroup.com

Attorney for Plaintiff